LC Paper No. CB(2)2198/05-06(01)

政 府 總 部
香 港 下 亞 厘 畢 道

GOVERNMENT SECRETARIAT
LOWER ALBERT ROAD
HONG KONG

本函檔號 Our Ref.: SBCR 3/2/3231/94
來函檔號 Your Ref.: PCO(O)115/156 pt.12

電話號碼 TEL. NO.: 2810 2666
傳真號碼 FAX. NO.: 2523 1685

29 May 2006

Mr Roderick B. Woo, JP
Privacy Commissioner for Personal Data
12/F, 248 Queen's Road East
Wanchai
Hong Kong

Dear Mr Woo,

Interception of Communications and Surveillance Bill

Thank you for your letter of 25 April 2005. On the points on which you have kindly provided your elaboration therein, we have the following observations.

Type 2 surveillance

We agree with your assessment that the scenario covered by paragraph (b) of the definition of "Type 2 surveillance" – i.e. the carrying of a covert surveillance operation with the use of an optical surveillance device or tracking device which does not involve entry into premises without permission or interference with the interior of any conveyance or object without permission – is not necessarily without privacy concern. Accordingly, we also consider it appropriate to require the operation to be sanctioned by an authorization under the Bill. However, we consider that any privacy concern would be of a lesser degree than the use of a listening device under the circumstances in question. Hence, executive authorization is proposed under the Bill. We note that in the US the use of optical device for covert surveillance is not statutorily regulated, and the Australian legislation requires judicial authorization for such operations if they involve entry into premises without permission or interference with the interior of any conveyance or object without permission (as we do under our Bill), but does not require authorization if such operations do not involve such entry or interference.

As regards the two scenarios covered in paragraph (a) of the definition of "Type 2 surveillance", they concern situations of participant monitoring, where the covert surveillance is carried out with the involvement of a consenting party. This participant can be an undercover law enforcement officer, an informer, or a victim of crime seeking assistance from a law enforcement agency. As the "participant" is expected by the target to hear the conversation or see the activities in the circumstances, he can relay what he has seen or heard to a third party anyway, and therefore we consider that the concern would be more on breach of confidentiality rather than infringement of privacy. This analysis is in line with court rulings in other common law jurisdictions. The difference between (i) and (ii) is merely technical — in both cases, the party to the conversation or the activities has no objection to the conversation or the activities being heard or seen , but under (i) the device is used by the "participant" himself while under (ii) the device is used by others with appropriate consent. We are of the view that the degree of infringement of privacy would not be substantially different between the two scenarios, and they should be subject to the same level of authorization (i.e. executive authorization).

We have discussed related issues with the Bills Committee, and you may wish to refer to the note attached at **Annex A** on our proposed framework on covert surveillance.

Device retrieval warrant

As explained previously, in general, it is envisaged that the devices should have been retrieved before the expiry of an authorization. Device retrieval warrants are only necessary when for operational reasons the devices cannot be retrieved before an authorization expires. Once the authorization has expired, law enforcement officers would no longer be authorized to use the device. The Administration would take a very serious view of any officer conducting interception or covert surveillance without proper authorization (including when such authorization has expired or has been revoked). The officers concerned could be subject to disciplinary actions — resulting in dismissals in the most serious of the cases, besides criminal sanctions. In practice, we believe that in order to maintain the covert nature of the operations in question, the law enforcement agencies (LEAs) would have every incentive to retrieve the device as soon as practicable.

Code of Practice

As we have explained to the Panel on Security and the Bills Committee, LEA officers who fail to comply with the new legislation could be subject to disciplinary action (which could range from verbal warning at one extreme for minor breaches to dismissal at the other extreme for very serious breaches) or, depending on the cases, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law.

A clause in line with section 13(2) of the Personal Data (Privacy) Ordinance (PDPO) regarding the admissibility of evidence in proceedings under the PDPO, in relation to a breach of the Code, may not have much relevance in our Bill. Unlike the PDPO, there is no criminal sanction under our Bill. A breach of the requirements under Bill would instead likely to be considered by the proposed Commissioner on Interception of Communications and Surveillance (the Commissioner) under the Bill in carrying out his review or examination function, apart from any disciplinary/criminal actions to be taken by the Administration in respect of the officer(s) concerned. This would already take into account the compliance with the Code of Practice, without the need for an "admissibility" provision.

In any case, we would make it abundantly clear to LEA officers the serious consequence of any breach of the relevant requirements. We shall include provisions in the Code to clearly set out the possible consequence of such breaches. The Code would be published and made public. Furthermore, under the Bill, the Commissioner would already be apprised of actions to be taken by the LEAs in respect of non-compliance. The head of the LEA concerned is also required to provide a report with details of any measures taken by the department concerned to address any of the issues arising from the decision of the Commissioner following his reviews or his examinations pursuant to complaints. We envisage that these details will include, where applicable, actions by the department in respect of the officers concerned. The Commissioner may further report cases of irregularity to the Chief Executive (CE), or the Secretary for Justice. Statistics on such cases would also be provided to CE in the Commissioner's annual report, which would be tabled in the Legislative Council (LegCo) for public scrutiny. These are powerful measures to ensure that LEAs and their officers will comply with the law and the applicable procedures.

I hope the above has clarified our thinking on the issues in question. You may also wish to note that we have recently issued our detailed response to the written submissions received by the Bills Committee on the Bill, including that from your goodself. A copy of our response as presented to the Bills Committee is attached herewith at **Annex B** for your reference.

May we thank you again for your useful comments on our legislative proposal.

Yours sincerely,

(Stanley Ying)
for Secretary for Security

c.c.

Clerk to Bills Committee	(Attn : Mrs Sharon Tong)
Department of Justice	(Attn : Mr Ian Wingfield)
Secretary for Home Affairs	(Attn : Ms Joanna Choi)

Annex A

Types of Covert Surveillance

Options for regulatory framework

In formulating our proposal for covert surveillance we have taken into account the discussion and recommendations in the 1996 consultation paper "Privacy : Regulating Surveillance and the Interception of Communications" of the Privacy Sub-Committee of the Law Reform Commission (LRC) (the 1996 LRC paper). In addition, we have taken reference from the regulatory regimes of comparable common law jurisdictions, in particular, that of Australia.

2. The **1996 LRC paper** recommends a regulatory framework comprising **three criminal offences** along these lines –

(a) entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein;

(b) placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier; and

(c) placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring without the consent of the lawful occupier either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant.

The 1996 LRC paper further recommends that **warrants be required to authorise** all surveillance within the scope of the proposed criminal offences.

3. On paragraph 2 (a), currently law enforcement agencies (LEAs) are already liable for trespass and any unlawful act that they may do on

the premises that they have trespassed. In practice, therefore, such operations are unlawful unless authorized under the law, e.g., by way of a search warrant. Our proposed legislation corresponds to the other two proposed criminal offences in paragraph 2 above, and other situations not discussed in detail in the 1996 LRC paper.

4. The regulatory regimes of **comparable common law jurisdictions** vary considerably. The United States (US) statutory regimes cover only the use of devices to monitor and record communications. The UK's statutory regime is more up to date and comprehensive, covering intrusive surveillance (where private premises are involved) and directed surveillance (covert surveillance other than intrusive surveillance). The UK regime provides for executive authorization of directed surveillance operations and approval of executive authorizations by a Surveillance Commissioner, who must be a sitting or former judge, of intrusive surveillance operations. We have taken greater reference from the legislation Australia enacted in 2004, which is the latest model among the jurisdictions that we have studied. Previously Australia's Commonwealth legislation covered only the use of listening devices. The 2004 legislation covers listening, data surveillance, optical surveillance, and tracking devices.

Our proposed regime

Definition of covert surveillance

5. We propose that our new legislation regulates surveillance carried out for any specific investigation or operation if the surveillance is –

(a) systematic;

(b) involves the use of a surveillance device; and

(c) is –

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

  (ii) carried out in a manner calculated to ensure that the person is

unaware that the surveillance is or may be taking place; and

(iii) likely to result in the obtaining of any private information about the person.

All such surveillance would require prior authorization under the proposed new legislation.

Types of authorization required

6. As different devices capture different types of personal information, their use affects privacy in different ways. The authorization scheme seeks to take this into account.

7. ***Listening devices and data surveillance devices*** capture the content of communications, or data in or generated from data-processing equipment, which may include communication data.

8. If access to the communication is already available through the presence of a person known by the target to be accessing that information, arguably there is little intrusion into the privacy of the other parties to the conversation. For illustration, if two persons (A and B) are engaged in a conversation, and A intends to repeat the conversation to an LEA, he may do so whether he has used a device or not. B knows full well of A's presence and the possible risk of A repeating the conversation to others. In both the US and Australia, for such "participant monitoring" no warrant is required. However, for tighter protection, we propose that **where a device to pick up or record the conversation is used whilst A and B are having the conversation, and A agrees to the use of the device in his presence, the LEA would need executive authorization**.

9. If, however, A is not present at the conversation but has arranged to plant a device to pick up or record the conversation between B and C, neither B nor C would expect that their communications would be picked up by A. The intrusion into privacy in respect of B and C would be much greater (unless the conversation takes place in circumstances that do not involve a reasonable expectation of privacy on the part of B, e.g.,

if he shouts across the street to C when there are other parties around). **If an LEA wishes to pick up or record the private conversation through the use of a device without a participating party, that operation would need judicial authorisation.**

10. ***Optical surveillance devices and tracking devices*** capture data which are different from the oral communications captured by listening devices. As the nature of the data involved is different, the privacy analysis is different, and the authorization criteria have to be adjusted accordingly.

11. In Australia, the use of optical surveillance devices other than in circumstances involving entry onto premises without permission or interference with any vehicle or thing would not require a warrant. We propose a tighter regime –

(a) a covert surveillance operation involving **the use of an optical surveillance device in a participant monitoring situation in places to which the public does not have access should require an executive authorization;**

(b) **the requirement for executive authorization should extend to the use of an optical surveillance device to monitor or record activities in places to which the public does not have access *provided that* such use does not involve entry onto premises or interference with the interior of a conveyance (e.g., a car) or object without permission**; and

(c) where **the use of the optical surveillance device involves entry onto premises or interference with the inside of a conveyance or object without permission, but does not involve a participant monitoring situation, judicial authorization would be required** in view of the greater intrusion.

12. For illustration, if a person (A) is in his own room and has drawn the curtains of the room, he can reasonably expect that what he does in

the room would be private. If an LEA wishes to enter the room to install an optical surveillance device before the person enters that room, that operation would need judicial authorisation (paragraph 11(c) above). If, however, A allows B into the room to observe what he does, and B covertly videotapes the scene, executive authorization would be required (paragraph 11(b) above).

13. A **tracking device** captures the location data of a person or an object. The collection of such data where the person or object moves in a public place should not pose much privacy concern, since one should not have much expectation of privacy with respect to his whereabouts in a public place.

14. In Australia, the use of a tracking device not involving entry onto premises without permission or interference with the interior of a vehicle without permission requires executive authorization. Otherwise a judicial warrant is required. We propose a similar regime –

(a) **if a tracking device is used in circumstances not involving entry onto premises without permission or interference with the interior of a conveyance or object without permission, it would require executive authorization**; and

(b) **if the use of a tracking device involves entry onto premises without permission or interference with the interior of a conveyance or object without permission, the operation would require judicial authorisation** because of the greater intrusion.

15. For illustration, if a tracking device is covertly placed inside a person's briefcase in order to track his movement, judicial authorization would be required (paragraph 14(b) above). If, however, a tracking device is placed on the outside of a conveyance and may hence lead to its driver's movement being traced, it would require executive authorization (paragraph 14(a) above).

Annex B

For information
25 April 2006

SB Ref: ICSB 7/06

Bills Committee on the Interception of Communications and Surveillance Bill
Administration's Response to Submissions to Bills Committee*

General Principles

	Issue	*Response*
1	Interception and covert surveillance are important investigatory tools. (preamble of DAB's submission)	We agree with the comments.
2	The regime should balance the protection of security and law and order; and safeguarding privacy. (preamble of DAB's submission; point 1 under "Strengths of the Bill" of Liu's submission)	We agree with the comments and the Bill seeks to achieve this aim.
3	The Bill is compliant with Article 30 of the Basic Law. (point 2 of Chan's submission)	We agree with this observation.
4	The Bill has introduced a number of safeguards and would not infringe on privacy of the public. (point 3 of Chan's submission)	We agree with this observation generally. Any infringement of privacy resulting from the carrying out of a covert operation duly authorized under the Bill would be reasonable and proportionate to a legitimate purpose.

Legend

Bar = Hong Kong Bar Association
Chan = Mr CHAN Chi-hing
DAB = Democratic Alliance for the Betterment and Progress of Hong Kong
HRM = Hong Kong Human Rights Monitor
Liu = Mrs Amy Y K Liu
Lam = Mr LAM Chi-wai
PCO = Privacy Commissioner for Personal Data
SOCO = Society for Community Organization

* The submissions are those made to the Bills Committee for its meeting on 3 April 2006.

	Issue	*Response*
5	The Bill is not compliant with provisions in the Basic Law and the International Covenant on Civil and Political Rights regarding the protection of privacy of communications; there are a lot of defects. (preamble of SOCO's submission) Reference from Canada, where there is a written constitution to protect human rights, should be drawn, instead of basing the Bill on the regimes in Australia and the United Kingdom (UK) (paras. 8-10 of Bar's submission).	We consider that the Bill complies with the human rights requirements prescribed in the relevant Basic Law provisions including those referring to the International Covenant on Civil and Political Rights. In addition, we have taken reference from relevant jurisprudence, including the decisions of the European Court and Commission of Human Rights and the practice of other common law jurisdictions including Canada.
6	The Bill should be enacted as soon as possible to avoid a legal vacuum. (point 1 of Chan's submission; preamble of Youth Action 21's submission)	We agree with the comments.
7	Subject of the Bill warrants more time for rigorous scrutiny. (paras. 6-7 of Bar's submission) Concerned over the lack of time to scrutinize the Bill. (para. 5 of HRM's submission)	We agree that there should be sufficient discussion in the society before we enact legislation on this important subject. In drafting the Bill, we have taken full account of previous discussions on the subject, e.g., the 1996 consultation paper of the Law Reform Commission (LRC) on interception of communications and covert surveillance, the 1996 LRC report on interception of communications, the 1997 White Bill on interception of communications, the 1997 Interception of Communications Ordinance and relevant court rulings. We have also been discussing with interested parties before and after the publication of the Bill. There have also been extensive media coverage and discussions on our legislative proposals published on 1 February 2006, on the Bill after its publication on 1 March 2005, on the five meetings of the Panel on Security of the Legislative

	Issue	*Response*
		Council (LegCo) on the subject, and on meetings of the Bills Committee. We will continue to work closely with LegCo to facilitate a thorough scrutiny of the Bill.
8	It is advisable to have a sunset clause to allow for scheduled systematic review and amendments. (para. 7 of HRM's submission)	We do not consider that a sunset clause is necessary. Like all other legislation, the Administration will monitor the operation of the Bill as enacted and review any areas of concern as and when necessary.
9	There was delay in legislation in the areas of interception and covert surveillance. (preamble of DAB's submission; para. 4 of HRM's submission)	Please see our response to item 7.
10	The Bill sets out a clear regulatory framework for public officers, with a two-tier approach, and provides a more comprehensive and unified regime. (points 2 and 3 under "Strengths of the Bill" of Liu's submission) Legislation in the area provides better checks and balances to prevent abuse. (preamble of Lam's submission)	We agree with these observations.
11	There is a need to legislate to protect privacy of individuals from being infringed by the media. (preamble of Lam's submission) Protection of the right to privacy against violations by private actors should be dealt with in future legislation. (para. 6 of HRM's submission) Administration should indicate when it would address the problems of non-government actors.	The infringement of privacy by non-government parties can be considered in the context of the LRC reports on covert surveillance, stalking, civil liability for invasion of privacy, and media intrusion.

	Issue	*Response*
	(para. 18 of Bar's submission)	
12	The Administration should address the issue of covert operations carried out by office holders of or on behalf of the state. (para. 16 of Bar's submission) All outside law enforcement agencies should not be allowed to conduct interception or surveillance activities in Hong Kong. (para. 26 of HRM's submission)	In line with advice that we have received in consultations, for the current exercise we seek to regulate the conduct of our law enforcement agencies (LEAs). As set out in our response to item 11, the activities of non-government entities can be covered in other contexts.
13	The Administration should address the problem of "exclusion" of persons acting on behalf of public officers. (para. 17 of Bar's submission)	Clauses 4 and 5 of the Bill clearly stipulate that no public officer shall, directly or through any other person, carry out any interception or covert surveillance. There would be no question of getting round the requirements of the Bill by "outsourcing".

Specific Provisions of the Bill

Clause 2 : Interpretation

	Issue	*Response*
14	Why a prescribed authorization for interception of communications may contain such broad terms, without any specific reference to communications (in paragraph (b) of the definition of "interception") that may be inspected under clause 29(1). (paras. 19-21 of Bar's submission)	Clause 29(1) contains detailed provisions for an authorization for interception. As for paragraph (b) of the definition of "interception", this is only a general definition included to facilitate reference throughout the Bill (i.e. the carrying out of intercepting act in respect of communications). The Bill contains provisions, such as clause 29(1) as read together with the condition provision in clause 3, etc., that will enable a specific

	Issue	*Response*
		authorization to be issued. Indeed, Schedule 3 expressly requires such details as the identity of the target, particulars of the addresses etc. to be provided if known, although it may not be possible in some cases (e.g. kidnapping cases). It is clear that under the Bill each case will be considered on its own merits, and the Bill is not too broad in this regard.
15	The Administration should clarify whether "intercepting act" covers broadband telecommunications service and mobile phone / personal data assistants. (paras. 22-24 of Bar's submission) Interception of communications through the internet, wireless telecommunications, e-mail, SMS message of mobile phones should be included as interception rather than covert surveillance. (part 2 of SOCO's submission)	The term "telecommunications interception" means "interception of any communication transmitted by a telecommunications system". The term "telecommunications system" has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance, i.e., "any telecommunications installation, or series of installations, for the carrying of communication by means of guided or unguided electromagnetic energy or both". Broadband transmission should therefore be covered if the other elements of the definition of interception act are also present. The same applies to other data transmitted by telecommunications (e.g. mobile phone and e-mail services).
16	Definition of "serious crime" is far too broad, and would cover offences under Public Order Ordinance, etc.. It should cover only the most serious crimes. The Administration to explain why the term is not defined by way of a list of enumerated offences. (paras. 47-54 of Bar's submission)	As previously explained, the serious crime threshold is but an initial screen. The other tests set out in the Bill, most importantly proportionality which in turn relates to the gravity and immediacy of the serious crime to be prevented or detected, must be met as well. We consider that for the purpose of an initial screen, making reference to the maximum penalty level is appropriate. A summary of our explanation provided to the Security Panel in this regard is at Annex A4 to the Bills Committee paper SB Ref: ICSB 1/06.
17	Difference in treatment for Type 1 and Type 2 surveillance / Need for two tiers of authorization - strong justifications are needed for executive	The Administration has explained the difference between Type 1 and Type 2 surveillance in previous papers. A summary is at Annex A4 to the Bills Committee paper SB Ref: ICSB 1/06.

	Issue	*Response*
	authorization. (paras. 29-34 of Bar's submission) Executive authorization should be cancelled. (divisions 2 and 3 under part 3 of SOCO's submission) Surveillance when participating party is present and consented would be more intrusive when carried out by third parties. (first paragraph under point II of PCO's submission) All covert operations should be authorized judicially unless justified in accordance with international human rights standards. (para. 13 of HRM's submission) Should not require all covert surveillance operations to be authorized by judges as that would reduce efficiency of law enforcement. (point 1(1) of Youth Action 21's submission)	As explained in these previous papers, our Type 2 operations (which include "participant monitoring") are generally not regulated in the legislation of some of the common law jurisdictions, or are subject to executive authorization. Overall, our proposed statutory regime covers such operations more extensively, and subject them to more checks and balances than the other common law jurisdictions that we have studied.
18	Definition of "Type 2 surveillance" - tracking device "doubling up" as listening devices requiring lower level authorization. (para. 35 of Bar's submission)	Tracking device is defined as "any electronic device used to determine or monitor the location of any person or any object or the status of any object". There is a separate definition of "listening device". If a device has multiple functions, it would be the actual function to which the device is put that would determine the authorization required. Hence, judicial authorization would be required if the device proposed to be used by the LEA would actually be used as both a tracking device and a listening device during the operation.

	Issue	***Response***
19	Definition and operation of the test of "reasonable expectation of privacy" - the reference to "entitled to" would allow junior officers to circumvent the provisions of the Bill; this should be something that only the court can decide. (paras. 37 - 39 of Bar's submission) There is a need for a clear definition or benchmark of the term of "reasonable expectation of privacy" (to be covered in the Bill or the Code of Practice), and all surveillance without authorization (i.e. not involving "reasonable expectation of privacy") should be reported to the Commissioner on Interception of Communications and Surveillance (the Commissioner) to ensure proper decision by LEAs. (point 1 of PCO's submission) The term "reasonable expectation of privacy" needs a definition. (para. 14 of HRM's submission)	We agree with the LRC in its recent report on covert surveillance, that *"(i)t would not be possible to set out in the legislation all the circumstances in which a person would be entitled to a reasonable expectation of privacy"* (para 2.43)). We note that the LRC has also used the word "entitled" in this context. We consider that the use of the expression "entitled" is more appropriate as the test is applied in the context of an advance application before the reasonable expectation of privacy actually arises and therefore before any person ***has*** such reasonable expectation of privacy (cf. para.1.41 of the LRC recent report on covert surveillance). The test to be adopted in determining whether an individual is entitled to a "reasonable expectation of privacy" is an objective one, and reference could be made to the jurisprudence in other jurisdictions as well as the caselaw under the European Convention on Human Rights in making this assessment. The approving authorities and the Commissioner under our proposed regime can take reference from such jurisprudence. LEA officers will be properly trained, and when in doubt, seek legal advice. The Bill already sets out clearly the circumstances where authorization is required for LEAs to carry out interception of communications and covert surveillance. All applications, their results and the execution of authorizations would be subject to the Commissioner's review. We do not consider it necessary or practicable to report all instances of covert surveillance to the Commissioner even though the person affected does not have any reasonable expectation of privacy in the circumstances of the case.
20	Unsystematic surveillance should not be excluded from the authorization regime by confining covert surveillance to "systematic" ones. (para. 25 of	The qualifier is necessary to exclude immediate response to operational circumstances or cursory checks that form part of an LEA officers' routine operations, e.g., in the course of patrolling a public place.

	Issue	*Response*
	HRM's submission)	
21	Paragraph (b) of the definition of Type 2 surveillance would enable monitoring of words and activities of neighbours without entry and should require judicial authorization. (second paragraph under point II of PCO's submission)	Paragraph (b) of the definition under Type 2 surveillance applies only to the use of tracking and optical surveillance devices. An authorization for Type 2 surveillance does not authorize the installation of a device in adjacent premises to record the words spoken by the subject next door.
22	If the definition of "public place" is intended to include conveyances, it should include public transportation only; otherwise "public place" should be defined in terms of "place" rather than "premises". (paras. 2-3 under point 3 of DAB's submission)	Our intention is that "public place" should also include "public conveyances". As "premises" has been defined to include conveyance, the reference is appropriate .
23	To clarify, in respect of the definition of "premises", what is meant by "offshore" structure, and restrict premises to those within Hong Kong. (point 1 of Lam's submission)	An offshore structure is one that is offshore and thus is not erected on land. It would not be necessary to specifically restrict the premises to those in Hong Kong since the LEAs' enforcement powers would be defined by the jurisdictional rules of the respective legislation.
24	To clarify the provisions relating to permission for entry onto premises, in particular, entry under disguise (such as undercover). (para. 4 under point 3 of DAB's submission) There are grey areas concerning from whom the permission for entry into premises should be sought. (para. 16 of HRM's submission)	"Permission" for entry onto premises refers to the permission given by the person who has the authority to give such permission. Who may be able to give the permission may therefore vary from case to case. In an undercover operation involving entry onto premises, the determining factor of whether a judicial authorization or executive authorization is required is not whether there has been permission to enter onto the premises, but whether the situation involves participant monitoring. If, for instance, the agent leaves behind a listening device for picking up conversations conducted inside the premises after his departure, a judicial

	Issue	*Response*
		authorization would be required.
25	Providing that one will not be entitled to reasonable expectation of privacy in public places violates human rights; conversations on mobile phones in public may be monitored without authorization as a result. (paras. 40-46 of Bar's submission) The court should not be deprived of the chance to decide whether a person is entitled to privacy in such circumstances. This would also reduce unnecessarily the police's exercise of discretion. (para. 24 of HRM's submission)	Clause 2(2) of the Bill provides that a person is not regarded as being entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place. The term "activity" has been chosen to be clearly distinct from that of "words spoken" in the context of the Bill – with the latter used in the definition of "listening device" and the former used in the definition of "optical surveillance device" and further with both used as distinct references in paragraph (a) of the definition of "Type 2 surveillance". The Bar Association's example of conversations in a public place would not be caught by clause 2(2), but would be regulated under the general provisions of the Bill, including the definition of covert surveillance under clause 2(1), under which a person may be entitled to a reasonable expectation of privacy for his conversations in a public place.
26	Protection by clause 2(3) in respect of LPP is not adequate, and there is no threshold requirement before granting authorization which may interfere with communications involving LPP. The Bill should provide for a high threshold for such operations. No emergency applications should be allowed. Conditions should be imposed to minimise intrusion. Product should be inadmissible as evidence unless waiver is available. There should be provisions on destruction/disposal of products from inadvertent intrusion, and notification of all lawyers, etc. of the office/residence concerned. (paras. 70 - 83 of Bar's submission)	The Administration fully respects LPP and would not target information protected by LPP. A number of safeguards have been built in to protect LPP materials. Please see Bills Committee papers SB Ref: ICSB 2/06 (issue 2), 3/06 (issue 1) and 4/06 (issue 1). The suggestion to notify the clients before any operation involving lawyers and related staff would unavoidably defeat the purpose of the operation and cannot be accepted. Taking into account discussions at the Bills Committee, the Administration is preparing draft provisions to make the protection of LPP in the Bill more explicit.

	Issue	*Response*
	Clients should be notified before covert operations on lawyers or their staff. (point 1 under "other suggestions" of SOCO's submission)	

Clause 3 : Conditions for issue, renewal or continuance of prescribed authorization

	Issue	*Response*
27	There is no stipulation that panel judge or authorizing officer must be satisfied with matters of fact before authorization. (para. 66 of Bar's submission)	The conditions for issue/renewal or continuance of prescribed authorizations are already set out clearly in clause 3 of the Bill – clause 3(1)(a) sets out the purpose; clause 3(1)(b) requires that the authorization sought is proportionate; and the proportionality (and hence the necessity) test is then further elaborated by reference to the relevant factors (including the immediacy and gravity of the matter, and the likely value and relevance of the information to be obtained), and whether the purpose can reasonably be furthered by other less intrusive means. This would thus require the satisfaction of matters of fact. We cannot envisage that the authorizing authority would be satisfied with the stringent conditions for issuing an authorization if he has doubts on the matters of fact submitted in applications.
28	It is difficult to imagine what constitutes "public security" that would not be covered by "serious crime", and there is the question on the relationship with the term "state security" as understood in the Mainland and the term "national security" as understood in international human rights jurisprudence. The concept of public security should be left out of the Bill. (paras. 55-65	The approach of having a separate limb of "public security" is consistent with Article 30 of the Basic Law (BL30) as well as the practice in other jurisdictions. BL30 and practice in other jurisdictions clearly envisage crime investigation and protection of public security to be two distinct and legitimate grounds for the relevant authorities to inspect communications. We have explained the rationale for the present approach as well as the need for the limb at Annex A1 to the Bills Committee paper SB Ref: ICSB 1/06 as well as under issue 1 of paper SB Ref: ICSB 2/06. We have also

	Issue	*Response*
	of Bar's submission) To clarify the meaning of "public security" and whether this includes "national security". (part 1 of SOCO's submission) The concept should be clearly and narrowly defined. Political interception and surveillance should be expressly prohibited. (paras. 17-19 and 22 of HRM's submission) The Administration should explain how officers of departments would decide on whether a non-criminal matter would be within the statutory remit of their functions (e.g. role of Police under Police Force Ordinance). (para. 56 of Bar's submission) Given the Police Force Ordinance does not empower the Police to conduct any political surveillance, the concept of "public security" should be seen as crime prevention and detection. Such acts on "security grounds" should be confined to, e.g., prevention and detection of the offences of terrorist activities, and the concept of terrorist acts should be narrowed down. (paras. 20-23 of HRM's submission)	provided in Annex A to our paper SB Ref: ICSB 5/06 some examples of non-crime public security cases. We have explained why it would be difficult to define the term "public security" exhaustively. We are now actively following up on the suggestion of adopting an exclusion clause. Please see our paper SB Ref: ICSB 5/06.
29	There may be difficulties in administering the proportionality test by the executive, resulting in a lack of uniformity among judges and authorizing officers of LEAs in their consideration of	We appreciate the need to maximise consistency of standards. This is one of the reasons for our proposal for a panel of judges for authorizing the more intrusive operations of interception and type 1 surveillance. For the authorizing officers within LEAs, although they are not legally qualified,

	Issue	*Response*
	applications for authorization. (paras. 67-68 of Bar's submission)	they have the advantage of operational experience in such operations and would be guided by the Code of Practice and any legal advice to be given by the Department of Justice where necessary. There would also be both internal and external oversight. In particular, the Commissioner will carry out audit checks and will be able to provide guidance in respect of the balancing exercise through, say, making recommendations to the heads of department on the arrangements or Code of Practice. The proposed regime should enable expertise and experience to be built up.
30	Need for the reference to "in operational terms" in the proportionality test, which may result in bias in favour of the LEAs. (para. 69 of Bar's submission; first paragraph under point III of PCO's submission)	The reference to "operational terms" is included to ensure that the authorizing authority does not consider the proposed authorization in isolation, but as part of an overall operation. Since no two cases are identical, at the end of the day, there would inevitably be some exercise of judgement having regard to the circumstances of the case.
31	Necessity should be satisfied before proportionality is assessed. The Bill should provide that interception and covert surveillance should only be authorized if there are no other options. (point 1 of DAB's submission).	In assessing whether the proposed operation is proportionate to the legitimate aim pursued, the approving authority will necessarily have to consider the need to carry out the operation. In particular, clause 3(1)(b) requires the approving authority to consider whether the purpose sought to be furthered by carrying out the interception or covert surveillance can reasonably be furthered by other less intrusive means, and the immediacy and gravity of the serious crime or particular threat to public security is expressly stated to be one of the factors to be balanced against the intrusiveness of the operation. We consider that this would ensure that any interference with privacy would not be arbitrary.
32	The Bill should provide for tests of reasonableness and necessity, and factors for consideration should include the previous duration of monitoring, gravity of the crime(s) involved and the possibility	The Bill has already stipulated the test of proportionality which includes the test for necessity. Factors such as immediacy and gravity of the matter, and whether there are less intrusive means, have also been built in. As far as Type 1 surveillance is concerned, the affidavit supporting the

	Issue	*Response*
	of using other investigative means. (division 2 under part 3 of SOCO's submission) Gravity of crime, place of intrusion, means of intrusion etc. should be considered in applying the proportionality test as recommended by the LRC report. (second paragraph under point III of PCO's submission)	application has to set out, *inter alia*, the form of the Type 1 surveillance (including the kind(s) of surveillance device(s) to be used), the particulars of the premises in which the surveillance is to be carried out (if known), the nature of, and an assessment of the immediacy and gravity of the matter, and the reason why the purpose cannot reasonably be furthered by other less intrusive means.
33	Unify the definition of serious crimes for interception and all covert surveillance operations by adopting the threshold currently proposed in respect of type 2 covert surveillance to avoid operational confusion. (point 2 of Lam's submission)	LEA officers are well trained and will have no difficulties in complying with the different thresholds in actual operations. The different thresholds for interception of communications and covert surveillance have taken into account the generally higher degree of intrusiveness of interception of communications.
34	Currently, there is no need for the applying officer to state in the application that he has "reasonable ground to believe" that an offence has been or is about to be committed, or that there is a threat to public security. The threshold on trying of other investigative means is lower than that in Canada and New Zealand. (paras. 105-109 of Bar's submission)	Clause 3 already requires that the immediacy and gravity of the serious crime or threat to public security and the availability of less intrusive means be taken into account in applying the proportionality test. This balancing approach is logical. For example, in cases where the threat, if materialized, is very grave, monitoring is justifiable even though the threat is not immediate. We note that Canada also adopts a similar approach, i.e., that the need to consider trying other investigative procedures does not apply to terrorism offences and crimes involving criminal organizations (Canadian Criminal Code 186(1.1)).

Clause 6 : Panel judges

	Issue	*Response*
35	Appointment of panel judges should be made by the Chief Justice (CJ) instead of the Chief Executive (CE). (division 1 under part 3 of SOCO's submission) Judges should have security of tenure and a 3-year appointment affects their independence; selection of judges should be left to the Judiciary/CJ. (paras. 11-12 of HRM's submission; point 2 under "Areas to be improved" of Liu's submission) CE is the appropriate authority for appointment (point 2 of Youth Action 21's submission).	We consider that CE should be the appointment authority, and have responded to the issue previously. A summary is at Annex A2 to Bills Committee paper SB Ref: ICSB 1/06. Briefly, panel judges are Court of First Instance (CFI) judges enjoying security of tenure. They are appointed by CE on the recommendation of CJ. They have the same powers, protection and immunities as a judge of the CFI has in relation to proceedings in that Court, and may be removed only on the recommendation of CJ and for good cause. The mere fact that they would be appointed for a period of three years would not affect their independence in discharging their statutory duties under the Bill.
36	Nature of "judicial" authorization is one of executive authorization by judges. Administration should explain why District Court judges are not appointed. In view of the constitutional position on the independence of the Judiciary, the conferral of non-judicial powers must be consented by the judge which should be detached from the court. Administration should justify the highest level of checking on the judge. (paras. 87-100 of Bar's submission) District Court judges could take up authorization of less intrusive operations. (para. 13 of HRM's submission) The provision that panel judges act judicially but are not regarded as a court makes it a fake judicial	We have responded to the issues regarding the need for a self-contained panel of judges at the CFI level, integrity checking arrangements, resource implications, and the meaning of the judges acting judicially. (Annexes A2, A3 and A11 to Bills Committee paper SB Ref: ICSB 1/06, issue 4 under paper SB Ref: ICSB 2/06, issue 2 under paper SB Ref: ICSB 3/06 and issues 2 and 3 under paper SB Ref: ICSB 5/06 are relevant.) The checking arrangement does <u>not</u> involve political vetting. In recommending a judge to be a panel judge, we envisage that CJ would necessarily take into account the willingness of the judge to serve as a panel judge.

	Issue	*Response*
	vetting. (division 1 under part 3 of SOCO's submission) Integrity checking may open up potentials for political checks and may affect judicial independence. (paras. 9-10 of HRM's submission)	

Clause 8 : Application for judicial authorization

	Issue	*Response*
37	Why application for judicial authorization should not be vetted and made by DoJ. (paras. 101-104 of Bar's submission)	The Bill seeks to set out clearly the requirements on the LEAs both before and after making applications for authorization. Clause 59 further provides for the making of a Code of Practice. All this should provide substantive guidance to LEA officers. As with other cases, where necessary, the LEAs will seek advice from DoJ. As such, we do not consider it necessary to mandate that all applications should be routed through or be made by DoJ.
38	Information to the panel judge must be fully particularized and meet a high threshold of assurance. Reference is made to the provisions in Canada and New Zealand. (paras. 110 - 113 of Bar's submission)	The information required to be provided in an application for judicial authorization is set out in Parts 1 and 2 of Schedule 3 to the Bill. There is no substantive difference between the provisions therein and those in overseas legislation quoted by the Bar in paras. 107 to 110 of its submission. It should also be noted that the particulars of the target may not be known in all cases. The Canadian and New Zealand examples quoted by the Bar also refer to "if known". The lists of information to be provided as set out in Schedule 3 to the Bill are already quite long and consist of the item of "if known, the identity of any person who is to be the subject of the

	Issue	*Response*
		interception". In any case, officers deliberately (or negligently) giving false information may be subject to criminal sanctions in addition to disciplinary actions.
39	Application for executive authorization is merely supported by a statement in writing (clause 14), giving it no assurance of reliability. (para. 15 of HRM's submission)	Officers deliberately (or negligently) giving false information may be subject to criminal sanctions in addition to disciplinary actions.

Clause 9 : Determination of application for judicial authorization

	Issue	*Response*
40	The judge should be required to consider and formulate the terms of his authorization to minimize the interference with privacy. (paras. 114-116 of Bar's submission)	The Bill imposes on the judge the duty to consider the proportionality and necessity of any authorization sought having regard to the degree of intrusiveness. Clause 31 of the Bill would already enable the judge to impose conditions in the authorization as he considers necessary to, *inter alia*, minimise the interference with the right to privacy.
41	It would be fair to give a right of appeal to the Commissioner of Police against a decision of authorization by the panel judge in some circumstances. (point 5 under "Areas to be improved" of Liu's submission)	The LEAs would carefully study the reasons for refusal given by the panel judge. In appropriate cases, if necessary, a new application with further and better particulars to address the judge's concerns could be made. We do not prefer a separate appeal mechanism.

Clauses 10 - 13 : Duration and renewal of judicial authorizations

	Issue	*Response*
42	The Administration must justify the 3-month authorization period proposed; in application for renewals, aggregate length of covert operation should be considered, and greater justifications should be required for cases where long period of operation has taken place. (paras. 117-121 of Bar's submission) Regulation of renewals should be strengthened. (division 2 under part 3 of SOCO's submission) Maximum number of renewals and more stringent criteria should be set. (point 3 under "Areas to be improved" of Liu's submission) Total duration of judicial and executive authorizations (including renewals) should be restricted to say 1 or 2 years. (points 3 and 4 of Lam's submission)	The 3-month period is only the maximum period and the authorizing authority may authorize an operation of a shorter duration. The period is comparable with the regime of other jurisdictions in this area. For renewal applications, Part 4 of Schedule 3 of the Bill already requires the applicants to provide additional information, stating whether the renewal sought is the first renewal and, if not, each occasion on which the authorization has been renewed previously, the value of information obtained so far, and the reason why it is necessary to apply for the renewal. Also the conditions for granting authorization under section 3 have already taken into account the intrusiveness of the operation. The approving authority needs to take into the account the above factors in approving the renewal. Setting the maximum number of renewal / maximum duration for the operations is not practicable. For example, serious and organized crimes may take a long time to plan, and hence long-term monitoring is required. The Commissioner would surely be interested in reviewing cases involving long term monitoring to ensure that the powers are not abused. We believe that these checks and balances built into our proposed regime will ensure that operations are not longer than justified.

Clauses 14 - 19 : Executive authorizations

	Issue	*Response*
43	Executive authorization to be subject to scrutiny of the court at some stage. (point 4 under "Areas to be	As a matter of principle, multiple renewals do not change the nature of the surveillance and therefore should not change the level of authorization required. As explained in our response to item 42 above, we consider that

	Issue	*Response*
	improved" of Liu's submission)	the many safeguards built in our proposed regime should already prevent abuse (e.g., the Commissioner would no doubt wish to review cases of multiple renewals and the number of renewals would be presented in the Commissioner's report). We therefore do not support changing the approving authority for Type 2 surveillance to panel judges only because of the number of renewals.
44	Why applications for renewals of an executive authorization should remain internal and not to be before a panel judge or some outside party. (para. 125 of Bar's submission) A ceiling on number of renewals (in particular in respect of executive authorizations) is to be set, or (in respect of executive authorizations) judicial authorization should be sought for subsequent renewals; and more stringent criteria should be needed for renewals. (point VI of PCO's submission)	Please see our response to items 42 and 43 above.

Clauses 20-28 : Emergency authorizations and oral applications

	Issue	*Response*
45	The Administration should justify its refusal to entrust emergency authorization to panel judges (bearing in mind applications may be made orally). "Loss of vital evidence" seems too broad to allow for emergency authorization. (paras. 131-135 of	Oral applications could apply to both judicial and executive authorizations, and are necessary where a written application is not feasible (e.g. where a panel judge may be contacted by telephone but a hearing is not feasible). Oral applications are subject to confirmation by the relevant approving authority within 48 hours.

	Issue	*Response*
	Bar's submission) Emergency applications should be made to the judiciary rather than the head of department concerned. Oral application should not be allowed and applications should be made to the judiciary. (divisions 4-5 under part 3 of SOCO's submission) Duration of emergency authorization should be limited to 24 hours. The Bill or the Code of Practice should give clearer definitions of terms such as "*imminent*" risk, "*substantial*" damage, "*vital*" evidence etc. in respect of emergency authorization to prevent abuse. Refusal for confirmation for emergency and oral authorizations should be reported to the Commissioner. There are insufficient safeguards against LEAs bringing upon themselves the urgency. (point V and third paragraph under point IV of PCO's submission)	On the other hand, emergency applications apply only to cases which would otherwise require judicial authorization. Under clause 20(1), this type of applications can only be made if it is not reasonably practicable to apply for judicial authorization (including oral applications to the panel judge) (e.g. urgent situations when authorization to conduct the operation is required as soon as possible) **AND** there is an imminent risk of death or serious bodily harm of any person, substantial damage to property, serious threat to public security, or loss of vital evidence. Emergency authorizations have to be confirmed by a panel judge within 48 hours. Both types of authorization are subject to the same conditions for authorization, internal review by the LEAs and oversight by the Commissioner. The ground of "loss of vital evidence" is one of the grounds for urgency in respect of emergency applications. In some cases, the loss of vital evidence is critical to the administration of justice, e.g., the destruction of a murder weapon. Other jurisdictions do not necessarily elaborate on what constitutes urgent or otherwise include similar elements in the legislation. It is difficult to give a legally exact definition of such concepts as "*imminent*" risk, "*substantial*" damage, "*vital*" evidence etc. Much depends on the circumstances of each case. We envisage that the Commissioner would naturally be interested in such cases and would monitor them closely to guard against abuse. On the duration of the emergency authorization, the Bill's proposal of 48 hours is the same as, or shorter than, the practice in Australia, UK and the United States (US). It takes account of the need to seek confirmation of the emergency authorization whilst not distracting resources to making the application for confirmation during the heat of the operation.

	Issue	*Response*
46	Oral applications should be allowed in urgent situations to ensure effective combating of crimes. (point 1(2) of Youth Action 21's submission)	We agree with the comments. An application for an emergency authorization may be made orally under the Bill.

Clauses 29 - 30 : Matters authorized, required or provided for by prescribed authorizations

	Issue	*Response*
47	The difference between "also authorizes" and "further authorizes" under clauses 29 and 30 – why the activities covered in clause 30(c), (d) and (e) are not authorized under the conscious decision of the relevant authority. (paras. 126 - 130 of Bar's submission)	There is a general difference in nature between the authorization items in clause 29 and those in clause 30. Some of the authorization items are necessarily case specific. For instance, in some cases, a postal interception may require the interception of communications made to or from the specified premises or address only; or the interception of communications made to or by any specified person only; or both. Each case therefore has to be considered on its own merits before a decision is made on what the authorization should authorize in the circumstances of the case. Clause 29(1) to (5) deals with such authorization items and further clause 29(6) and (7) deals with actions which are essential for carrying out the operations under those authorization items. Clause 30, on the other hand, authorizes what is essentially incidental conduct, i.e., the undertaking of any conduct which it is necessary to undertake in order to carry out what is authorized or required to be carried out under the prescribed authorization. For example, the retrieval of the surveillance device used in an authorized covert surveillance operation is part and parcel of the operation. It is therefore unnecessary to provide for each item to be separately authorized. However, any conduct is covered by the "further" authorization under clause 30 only to the extent that it is necessary or is required to carry out a prescribed authorization.

Clauses 32 - 37 : Device retrieval warrants

	Issue	*Response*
48	The application for the warrant should be mandatory to avoid undue delay in removing the devices, and a warrant duration shorter than 3 months should be considered. (part VII of PCO's submission) Stipulating a one-month period for retrieval warrants would be more appropriate. (point 5 of Lam's submission)	A prescribed authorization already authorizes the retrieval of devices under clause 30. Device retrieval warrants are only necessary where, for some reason, the devices cannot be retrieved before an authorization expires. Once the authorization has expired, law enforcement officers would no longer be authorized to use the device. The warrant duration of 3 months is only a maximum that the judge may approve, taking into account the practical difficulties in some cases to retrieve the device. The LEAs would have every incentive to retrieve the device as soon as practicable.

Clause 38 : The Commissioner

	Issue	*Response*
49	Same comments on the constitutional position of panel judges apply. The commissioner should be appointed from former judges to avoid appearance of serving judges reviewing the performance of other serving judges. (paras. 141-142 of Bar's submission) The Commissioner should be appointed from former Court of Final Appeal (CFA) or Court of Appeal judges. (division 1 under part 4 of SOCO's submission)	In order not to unnecessarily restrict the pool of candidates, we have provided in the Bill for both serving and former judges at the High Court level to be eligible for appointment as the Commissioner. Former permanent judges of the CFA would also be eligible. The Commissioner would perform his functions under the Bill outside of the Judiciary.

	Issue	*Response*
50	Given the Commissioner's access to considerable amount of sensitive information, there should be suitable regulation of his actions both during and after his service. (point 3 of Youth Action 21's submission)	The safeguards lie in CE making the appointment on CJ's recommendation, plus other procedural safeguards such as extended checking. Like others who are appointed to such positions of trust, the Commissioner is not expected to use the information to which he has access for purposes other than those related to his performance of his functions under the Bill, either during or after his service.

Clauses 40 - 41 : Reviews by Commissioner

	Issue	*Response*
51	To explain why report to Secretary for Justice (SJ) is needed when there is no criminal sanction for breach of the Bill. (last paragraph under part VIII of PCO's submission) Reports to CE and SJ should also be submitted to LegCo. (division 2 under part 4 of SOCO's submission)	While no criminal sanctions are provided under the Bill, there are existing offences (such as misconduct in public office) which may be applicable. The Commissioner may report to SJ for consideration of prosecution in cases of possible breach of existing laws. (Please see Annex A9 to Bills Committee paper SB Ref: ICSB 1/06 for examples of offences that may be involved.) By their confidential nature, such reports as well as other confidential reports to CE should not be made public.

Clauses 42 - 46 : Examinations by Commissioner

	Issue	*Response*
52	The threshold for application should be to "suspect" (rather than to "believe") that oneself is the target of an operation. (para. 143 of Bar's submission) The objective threshold of "reasonable ground to	We would be happy to consider the drafting issues at the clause by clause examination stage. We envisage that the Commissioner's staff will provide anyone who is in genuine need of assistance with practical advice as far as possible. However, we do not consider it necessary to make a statutory requirement

	Issue	*Response*
	believe" would prevent abuse. (para. 5 under point 2 of DAB's submission) The Commissioner should assist applicants in the complaint procedures, similar to the relevant provisions in the Personal Data (Privacy) Ordinance (PD(P)O). (first paragraph under part VIII of PCO's submission)	for the Commissioner to provide such assistance.
53	Examination to be carried out only on the basis written submission as laid down in clause 45(1)(b) is too restrictive, and denial of access to information by the applicant (as provided for in clause 45(2)) is not necessary. (part IX and fourth paragraph under part VIII of PCO's submission)	Due to the sensitive nature of the details involved in such covert operations, it is not appropriate for *inter partes* hearings to be carried out, nor to allow the applicant to access the relevant information. The provisions in question are aimed to protect the Commissioner from such demands of the applicant.
54	The test to be used in examination under clause 43(1)(b) and (2) should be "should have been, but has not been, ***applied for*** or renewed". (para. 144 of Bar's submission) With the wording of "should have been ..... issued or renewed", it is not clear whether this would cover the case where Clause 3 is not fulfilled and hence authorization should not have been given even if applications were made. (third paragraph under part VIII of PCO's submission)	The reference to "should have been" concerns whether the issuance of the authorization should have occurred given the operations carried out, rather than whether the conditions for issuance have been satisfied. The test of "should have been, but has not been, *issued* or renewed" (rather than "applied for") is appropriate. Otherwise, covert operations for which the application for authorization has been made but rejected would not be caught.

	Issue	*Response*
55	The Commissioner should not be constrained in his functions to principles applicable to judicial review (JR). (para. 146 of Bar's submission)	We have carefully considered if the JR test is appropriate for considering complaints. As a matter of legal policy, we consider that coercive orders should not be liable to appeal. The JR test seeks to avoid the merits of the authorization, as opposed to the compliance of procedures and other requisite requirements, being subject to appeal. The test is also consistent with that of the UK Investigatory Powers Tribunal in handling such complaints. We believe that this test is appropriate as the function of the Commissioner should not be that of an appeal body over the merits of the decision. While the Commissioner could not substitute his own decision for that of the original decision maker, the JR test would provide a sufficient safeguard against abuse of the system by the LEAs, by allowing the Commissioner to identify any cases in which operations have been conducted without proper authorization or where there has been procedural irregularity or the decision is so unreasonable as to be irrational.
56	Ceiling of compensation should be set. (point 6 of Lam's submission)	It would not be appropriate to set a ceiling. The Commissioner will determine the appropriate amount of compensation having regard to the actual circumstances of each case, such as the extent and duration of the intrusion and any aggravating or mitigating factors.

Clauses 47 - 50 : Reports and recommendations by Commissioner

	Issue	*Response*
57	The required content of the Annual Report is too limited. (paras. 147-148 of Bar's submission) Reports should be provided to LegCo. (division 4 under part 4 of SOCO's submission)	As a matter of fact, the list of information to be provided is already very long, taking into account relevant provisions in the 1996 LRC report on regulation of interception, 1997 White Bill and the Interception of Communications Ordinance 1997. Viewed in its totality, the information to be provided is comparable to, if not more than, that given in overseas

	Issue	*Response*
		jurisdictions. For example, we would require that information for interception of communications and covert surveillance be provided separately. Information on not only judicial but also executive authorizations would have to be provided. In determining the contents of the report, it would be necessary to balance between confidentiality and transparency. Revealing too much detail would expose our capability to criminals, thus allowing them to evade justice. There is therefore a limit to what may be published.

Clauses 51 - 52 : Further powers of the Commissioner and reports on non-compliance

	Issue	*Response*
58	The Commissioner should have powers to order the immediate cessation of operations / summon and examine witnesses. (second paragraph under part VIII of PCO's submission) Power of Commissioner to require public officer to answer question and provide information lacks teeth without provision of sanction. (fifth paragraph under part VIII of PCO's submission) In case of non-compliance with the Commissioner's requests, legal procedure should be available to ensure compliance. (point 7 of Lam's submission)	As explained in our response to item 55 above, it would not be appropriate for the Commissioner, a review authority, to be an appeal authority. Nonetheless, the Commissioner would have a statutory duty to notify the departments of the findings in his reviews and the determinations of his examinations in relation to the complaints. We expect that if the Commissioner notifies the LEA concerned of irregularities that merit cessation of the operations, the LEA would discontinue the operations. Clause 51 already empowers the Commissioner to obtain information from any person and to require officers to answer questions or provide information, or to prepare reports on operations carried out. We consider that the power is already sufficient. Any non-compliance may be reported to the head of departments, or CE / SJ as appropriate, and referred to in the Commissioner's annual report, which will be tabled at LegCo. We consider that the powers are already sufficient for the Commissioner to effectively discharge his duties.

Clause 55 : Discontinuance of interception or covert surveillance

	Issue	*Response*
59	Head of departments should inform Commissioner upon discontinuation of authorizations which are issued by mistake, such that notification can be carried out. (para. 4(ii) under point 2 of DAB's submission)	The suggestion is covered by clause 52 of the Bill, which already provides that any failure by the department or any of its officers to comply with any relevant requirements would have to be reported to the Commissioner. Clauses 41(2) and 46(2) also require the departments to report to the Commissioner the details of any measures taken by them to address any issues identified in the findings of the Commissioner's reviews and any issues arising from his determinations in relation to the complaints. As regards notification, we have previously explained the difficulties from an operational point of view (please see our response to item 70 below). Nonetheless, we are trying to see if any notification in limited circumstances is feasible.

Clauses 56 - 57 : Safeguards for protected products and record keeping

	Issue	*Response*
60	Provisions on the duration of retention and the manner of disposal of materials collected are not sufficiently detailed. To clarify if additional provision is needed to provide more control on the removal of materials from Hong Kong. (paras. 27 and 30 of HRM's submission)	The Bill provides many safeguards on the materials gathered and stipulates detailed record keeping requirements. Clause 56 sets out the safeguards for protected products, and clause 57 deals with record keeping. In particular, clause 57(1)(g) requires records to be kept to enable the Commissioner to perform his functions. We are also preparing amendments to these clauses to ensure that the protection of material subject to legal professional privilege is made explicit. The sharing of information with our counterparts in other jurisdictions is subject to applicable laws. For details, please see the paper prepared for the Panel on Security for discussion at its meeting on 3 January 2006.

	Issue	*Response*
61	Clause 56 does not explicitly address the question of making available product of operations with other departments or agencies in Hong Kong or elsewhere, the latter may be in furtherance of mutual legal assistance or otherwise. (paras. 165-166 of Bar's submission)	Please see our response to item 60.

Clause 58 : Non-admissibility of telecommunications interception products

	Issue	*Response*
62	The Bill clearly sets out the admissibility of information collected through interception and serves to save time and costs when the question of admissibility arises. (point 4 under "Strengths of the Bill" of Liu's submission)	We appreciate the comments. The Bill follows the UK practice in this regard. It could better protect privacy and safeguard sensitive information.
63	Notwithstanding the proposed non-admissibility of intercepts as evidence, the defence should have access to it and should be able to produce it as evidence to demonstrate innocence. The decision of disclosure should be left to the trial judge instead of the prosecutor. Intercepted materials should be disclosed unless covered by public interest immunity. Prohibition of asking questions concerning interception denies "equality of arms". Administration should explain how investigation relying on information obtained from prescribed authorization can be effectively	Annex A12 to the Bills Committee paper SB Ref: ICSB 1/06 elaborates on the proposed regime of evidential use of intercepted materials. The present provisions follow the UK practice in this regard. Specifically, the UK practice has been held to be consistent with the principle of "equality of arms" since neither the prosecution nor the defence have access to the actual product. In the event that exculpatory material is identified during the course of an investigation the directions of the trial judge will be sought and the judge may order disclosure of information.

	Issue	*Response*
	challenged, and power of the trial judge in excluding evidence. (paras. 153-163 of Bar's submission)	
64	The Bill has not dealt with the admissibility of unlawfully obtained interception or surveillance products. (para. 164 of Bar's submission)	As explained in the paper SB Ref. ICSB 4/06 presented to the Bills Committee (under issue 4), under our common law system, the admissibility of unlawfully obtained information / materials as evidence would be determined by the court balancing the probative value of the evidence and prejudicial effect on parties concerned. This would allow the court to make its judgment having regard to the unique circumstances of each and every case. We believe that this should continue to apply.

Clause 59 : Code of Practice

	Issue	*Response*
65	The Code of Practice should be laid before LegCo. The Administration should confirm if there is only one code. (paras. 151-152 of Bar's submission) That the failure to comply with any provision of the Code does not affect the validity of any prescribed authorizations (as provided for in clause 59(5)) overkills the effectiveness of the Code. (sixth paragraph under part VIII of PCO's submission) Clear operational guidelines should be given to front-line officers. (point 1 under "Areas to be improved" of Liu's submission)	The Code of Practice will provide guidelines to LEA officers for complying with the Bill. The Code will be published, and there will be only one Code. Clause 59 provides that it should be made by the Secretary for Security. Clause 59(5) provides that a failure to comply with any provision of the Code is for all purposes not of itself to be regarded as a failure to comply with any provision of the Ordinance. The formulation is similar to that in a number of codes of practice. This is not an "absolute exoneration". Indeed, there is a similar provision in the PD(P)O. In any case, the Commissioner has the general power to review compliance of departments with the "relevant requirements" (including the Code of Practice) and report to CE, SJ or the head of department as he deems appropriate.

Clause 61 : Immunity

	Issue	*Response*
66	The immunity provision of Clause 61 is too wide and only clause 61(1)(a) is acceptable. Interception made on a mistaken basis should not be an exception. (paras. 139-140 of Bar's submission) The proposed immunity would take away rights conferred under section 66 of the PD(P)O. (part X of PCO's submission)	It is important that honest mistakes would not attract liability. The clause is necessary not only to protect LEA officers in carrying out covert operations under the Ordinance, but also, say, acts carried out by the Commissioner, or acts carried out upon the request of the Commissioner to provide information to assist in his investigations, which would otherwise incur civil liability (such as breach of confidentiality) on the person providing the information. The immunity would not affect any liability arising from unauthorized entry onto premises and interference with property (clause 61(2)). Moreover, the Bill already provides for certain measures to guard against abuse. The note on "Sanctions and Code of Practice" at Annex A9 to Bills Committee paper SB Ref: ICSB 1/06 is relevant. The complaint and compensation mechanism under the Bill is designed to be a self-contained regime to provide redress to persons whose right to privacy is breached by unlawful covert operations. Given the covert nature of these operations, it would be more appropriate for the issue of compensation to be dealt with by the new regime under the Bill rather than under section 66 of the PD(P)O. In any case, the right of an aggrieved individual to bring an action under the Hong Kong Bill of Rights Ordinance for breach of his right to privacy under Article 14 of the Bill of Rights would not be affected.

Clause 65 : Transitional arrangements

	Issue	*Response*
67	Application of clause 58. (paras. 167-168 of Bar's submission)	The inadmissibility provision under clause 58 would better protect the privacy of the parties previously intercepted, as explained in Annex A12 to the Bills Committee paper SB Ref: ICSB 1/06. Since the same privacy and policy considerations apply, we consider it appropriate to apply the safeguard to pre-existing intercepted materials.

Schedule 5, Clause 5 : Consequential amendments to Telecommunications Ordinance

	Issue	*Response*
68	The Administration should justify the proposed new section 33 of the Telecommunications Ordinance (TO) under which CE alone is given the power to intercept without safeguards on oversight, and use and disclosure of data. The Administration should ensure that any interception is subject to proper authorization and oversight. (paras. 25-28 and 169 of Bar's submission)	Section 33 of the TO currently reads – *"Whenever he considers that the public interest so requires, the Governor, or any public officer authorized in that behalf by the Governor either generally or for any particular occasion, may order that any message or any class of messages brought for transmission by telecommunication shall not be transmitted or that any message or any class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order".* Under this section, the CE may, when he considers it to be in the public interest, order the interception of telecommunication messages, including both what is normally understood to be the "contents" and the "non-contents" parts of the messages. In the judgment of the CFI in February 2006 on the constitutionality of the section, the court declared that **insofar as that provision authorizes or allows access to or disclosure of the contents of any message**, it is unconstitutional. In line with the

	Issue	*Response*
		judgment of the CFI on the constitutionality of the provision, which has not been a subject of further appeal, we have proposed to amend section 33 of the TO as currently provided for under clause 5 under Schedule 5 of the Bill. The amended section 33 of the TO proposed in the Bill seeks to preserve that part of the provision that has not been ruled unconstitutional by the court. This is required to enable, for example, the Office of the Telecommunications Authority (OFTA) to undertake its investigations into contraventions by unlicensed operators of international calls under the Telecommunications Ordinance, as well as to enable the execution of prescribed authorizations when they are issued. We have taken the opportunity to provide safeguards in the amended provision. First, instead of relying on the usual meaning of "contents", i.e., the communication part of a message, we have borrowed the same broad meaning of "contents" as in the Bill, i.e., "the contents of any communication transmitted by a telecommunications system include <u>any data</u> produced in association with the communication" (emphasis added). Then the revised section 33(2) makes it clear that an order shall not of itself authorize the obtaining of contents of any individual message. Hence, the order to be made by CE under this revised provision cannot authorize the obtaining of <u>any data</u> (voice and other data) in association with any individual message. There would be no interference with any privacy of communication. Further, the revised provision stipulates that no data about any individual message may be <u>obtained</u> (revised section 33(2)). There is therefore no question of the messages being recorded and <u>stored</u> by way of the order. There would therefore be no interference with the privacy of communications.

Schedule 5, Clause 7 : Consequential amendments to Personal Data (Privacy) Ordinance

	Issue	*Response*
69	Amendments to PD(P)O cannot be accepted in view of the need for a notification mechanism. (para. 170 of Bar's submission) The amendment should be made an independent provision if the intent is to have no overlap with the jurisdiction between the Bill and PD(P)O. (part XI of PCO's submission)	The amendments seek to avoid duplication of purview between the Privacy Commissioner for Personal Data and the Commissioner under the Bill. We will consider the drafting points raised at the clause-by-clause stage.

Other Issues

	Issue	*Response*
Notification of targets		
70	Objects of authorizations must be informed so that they can decide to pursue whatever remedy is available; the unavailability of information about such operations to the target would make it difficult to him to seek JR or lodge application to the Commissioner for examination. (paras. 136-138 and 149-150 of Bar's submission) Persons affected should be notified by the Commissioner when he finds that covert operations were carried out without authorization during review, or heads of department discontinue an operation due to authorization by mistake. (paras. 1-4 under point 2 of DAB's submission)	The grounds against a general notification mechanism are explained in Annex A7 to the Bills Committee paper SB Ref: ICSB 1/06. Nevertheless, taking into account views that we have collected, we are considering whether it is feasible to have some form of notification in limited circumstances.

	Issue	*Response*
	Notification should be made within a reasonable time after the operation, whether or not prosecution is initiated. (division 3 under part 4 of SOCO's submission) Absence of notification would not provide sufficient protection for targets whose privacy rights might have been wrongly infringed; redress channel not meaningful without notification. To consider notification to be allowed at least for limited categories of cases. (part IV of PCO's submission) To consider the possibility of disclosure of wrongful acts when it would not undermine law enforcement. (para. 29 of HRM's submission) Notification would be prejudicial to investigation efforts. (point 1(4) of Youth Action 21's submission)	
Sanctions for non-compliance		
71	Non-compliance with any substantive provisions of the Bill should be made a criminal offence. (paras. 84-86 of Bar's submission) There should be criminal sanctions for breach of the Bill. (point 2 under "other suggestions" of SOCO's submission; para. 28 of HRM's submission) Criminal sanctions would reduce the law	Please see Annex A9 to the Bills Committee paper SB Ref: ICSB 1/06. Please also see our response to item 51 above.

	Issue	*Response*
	enforcement efficiency of the public officers; disciplinary actions would be more appropriate. (point 1(3) of Youth Action 21's submission)	

Security Bureau
April 2006