For information
10 June 2006

SB Ref: ICSB 10/06

Bills Committee on the Interception of Communications and Surveillance Bill
Administration's Response to the issues raised in the submission from the Law Society of Hong Kong on 16 May 2006

Issue	***Response***
1. Covert Surveillance : Activities in Public Places	
"Activity" should be defined clearly to ensure that it does not cover conversations, by inserting a suitable definition clause.	We have explained in the paper ICSB 6/06 the intention behind the clause. We would further consider making the intention more express.
It is not right to define in local legislation that one can never have an expectation of privacy in a public place. In particular, the definition of "*public place*" could include a restaurant and even a private room in a restaurant, where one would have an expectation of privacy. Excluding all activities carried out in a public place from the operation of the Bill contravene human rights.	In line with the jurisprudence in common law jurisdictions such as the US, a person whose activities are in the plain view of the public is not entitled to a *reasonable* expectation of privacy of not being seen by others. A private room at a restaurant would not be regarded as a "*public place*" since it is not a place to which the public have access under section 2 of the Summary Offences Ordinance. In any case, the definition in the Bill is for the purpose of authorization under the Bill, and would not affect the general rights of the persons.
2. Type 2 surveillance : participant-monitoring surveillance	
Participant-monitoring surveillance still intrudes into privacy even where undercover agents use covert surveillance devices. By-passing judicial authorization for all participant-monitoring may allow the LEAs to circumvent an accused's right	As explained in previous papers (a summary is at Annex A4 to the Bills Committee paper SB Ref: ICSB 1/06), in a number of common law jurisdictions, our Type 2 operations (which include "participant monitoring" when there is a reasonable expectation of privacy) are generally not regulated in legislation or are subject to executive authorization. Overall, our proposed statutory regime covers such

Issue	*Response*
to silence and their corresponding duty to caution an accused before soliciting information from him.	operations more extensively. The right to silence relates to the right to fair trial, which is a separate issue. The right of the accused to silence will be addressed by the trial judge, when considering the admissibility of the product of participant monitoring. The duty to administer caution only applies to specific circumstances by an LEA officer when the suspect is under arrest. This would not apply in the case of covert operations.
3. Conditions for Prescribed Authorization : Public Security and Serious Crime (Clause 3)	
The term "*public security*" is vague and should be left out of the Bill, unless a clear definition is inserted. Examples given by the Administration on non-crime *"public security"* cases can be covered by deeming "serious crimes" to include acts committed or to be committed outside Hong Kong, which would have constituted a serious offence in Hong Kong had the acts taken place inside Hong Kong. An exclusion clause does not provide a satisfactory solution to the problem. Without a clear definition and statutory guidance, the authorizing authority would have great difficulty in coming up with a proper and consistent approach as to what constitutes *"public security"* in the context of the Bill.	Our approach to the issue has been explained in detail in the paper SB Ref: ICSB 8/06. The solution proposed addresses crimes which may be committed elsewhere, but does not facilitate the monitoring of possible threats to public security at a stage before any particular offence is in contemplation or is only in a preparatory stage. We share the concern to ensure a consistent approach in handling authorizations, including those in the area of public security. One of the reasons for setting up a panel of judges to consider applications is exactly to allow them to build up expertise and consistency. For less intrusive operations, authorizations are given by senior LEA officers who are experienced in the area.

Issue	*Response*
4. Conditions for Prescribed Authorization : Threshold for findings	
A threshold should be set as the proposal envisages authorization being granted by a CFI judge. The applicant must provide "reasonable grounds" on oath in support of the application.	The conditions for issue/renewal or continuance of prescribed authorizations (including the proportionality test) are already set out in clause 3 of the Bill. The threshold test is only appropriate where there are facts to be determined on an objective basis, e.g. for search warrants that there is evidence of an offence in certain premises. In our proposed regime for covert operations, the test is more complex and the judge is both objectively determining the existence of certain facts and satisfying himself that certain prerequisite conditions are met. In any event, 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. See also our response to Issue 5 below.
5. Conditions for Prescribed Authorizations : the Proportionality Test	
The reference to "*in operational terms*" under clause 3(1)(b)(i) should be deleted. The Administration's intention would be better reflected by using the phrase "*balancing, in the context of the overall operation, the relevant factors …*". The relevant factors should be balanced against other fundamental rights, besides privacy, e.g. the right to LPP and the right to silence. The balancing exercise should therefore also cover "*other rights and obligations that may likely be infringed*".	We have discussed similar issues with the Bills Committee, and we would review the elements contained in the provision and revise the wording as appropriate.
LRC's test that "there is reasonable suspicion that an individual is committing, has committed, or is	We discussed related issues with the Bills Committee on 2 June, and will consider whether it is appropriate to refer to the concept of "reasonable suspicion" in the

Issue	*Response*
about to commit, a serious crime, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong" should be adopted, and the 14 items listed in paragraph 4.4 of the LRC Report should be specifically included in an application for a prescribed authorization.	conditions for prescribed authorizations.
6. Panel Judges and Security Clearance	
The Panel judges would be dealing with administrative applications virtually on a full time basis and so they would be acting administratively rather than judicially. As the regulatory scheme needs a maturing authorizing body, District Court judges should be excluded. The scheme should apply to all CFI judges. It is inappropriate for the CE to make appointments to the Panel as there should be a clear separation of functions between the Executive and the Judiciary. The additional security clearance for panel judges will set a bad precedent.	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.) Indeed, as explained in the paper presented to the Security Panel for discussion on 2 March 2006, the powers of CE under Article 48 of the Basic Law (BL48) include, inter alia, the power to appoint and remove judges of the courts at all levels. BL 88 further provides that the judges of the court 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 Hong Kong Special Administrative Region. Our current proposal for CE to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance is in line with that role. The working arrangements for the panel judges would be determined by the Judiciary. The work as panel judges would not affect the discharge of their duties as CFI judges. In any event, to have a distinct panel of judges as proposed would enable the Judiciary to ensure that the judges concerned do not handle criminal cases – so that the question of being "prosecution minded" should not arise.

Issue	*Response*
7. Applying for Judicial Authorization	
The information and the facts sought to be asserted before a judge must be fully particularized and meet a high threshold of assurance. The deponent must provide "*reasonable grounds as to belief*" in the affidavit. The deponent should support the application by particulars and indicate whether the informant has provided reliable information in the past. The identity of informants must be protected and should be handed to the judge in a sealed envelope.	See our response to Issues 4 and 5 above. Similar to the handling of any sensitive information, the LEAs would take appropriate measures as necessary to protect information regarding the identity of informants participating in covert surveillance operations under the Bill.
8. Determining an Application for Judicial Authorization	
There should be provisions requiring a judge to consider and formulate the terms of his authorization to minimize the interference with the right to privacy. Any authorization should be for a minimum period with minimum interference.	As explained in our response to the Bar on the point, 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, and clause 31 of the Bill already enables the judge to impose conditions in the authorization as he considers necessary to, *inter alia*, minimise the interference with the right to privacy. (Please see below on the issue of duration of authorization.)
9. Duration and Renewal of Judicial Authorization	
There should not be a blanket 3-month period. Authorization given should be "*the minimum necessary*" to minimize intrusion into privacy.	As explained in our earlier response to the submissions, the 3-month period is only the maximum period. The duration of the authorization sought is necessarily one of the matters to be taken into account by the issuing authority who may issue the

Issue	*Response*
The authorizing judge should consider factors such as the aggregate amount of time and the need for more information. The initial authorization should end at the time when the suspect is alerted to the investigations (i.e. upon arrest or contact by the LEAs). If the LEAs wish to continue to intercept communications of the suspect, they need to seek fresh authorization.	authorization for a lesser period by varying the terms of the authorization applied for. The maximum period proposed in the Bill is comparable with the regime of other jurisdictions in this area. Clause 55 already provides that once the conditions for continuance with an authorization no longer exist, LEAs would have an obligation to discontinue the operations. A fresh application will have to be sought in such case to continue the operation. Also, in case the circumstances change dramatically, such as the investigation pursuing a different area of criminal conduct, a new authorization will be sought and at that time the likelihood of picking up LPP material will be revisited in the context of the circumstances revealed by the fresh application.
Renewals of applications should not be automatic. When applying for an extension, there must be a full disclosure of all the relevant information to the judge, including the likelihood of interception of conversations subject to legal professional privilege. The LEAs must cite any additional grounds.	Renewals are not automatic and would be authorized only upon application. The authorizing authority would need to be satisfied with the same stringent conditions before renewal is granted, and in addition, further information (such as the value of information obtained) needs to be provided by the LEAs in a renewal application. There is no question of "automatic" renewals.
10. Executive Authorizations	
The aggregate period of renewals should not exceed the maximum period permitted under the 1st authorization. Beyond the maximum period, a new application is required. If a suspect has been arrested he has a right to remain silent and once this right is in place there should be a statutory requirement for additional authorization of continued interception.	Renewals must satisfy the same conditions for authorization as a new application. Requiring a fresh application rather than a renewal provides no additional safeguards. And as aforementioned, the right to fair trial is a separate issue. Such rights exist independent of whether or not a person is under arrest. The Bill has already stipulated criteria for discontinuation of operations under Clause 55 if the conditions for the continuance of the prescribed authorization are not met, or when the purpose of the authorization has been achieved. See also our response to Issue 9 above.

Issue	*Response*
A judge should authorize all renewals. The Administration must explain why it proposes applications for renewals of executive authorizations should not be subjected to external review.	In our Bill, the question of whether to have a judicial or executive authorization is determined by the degree of intrusiveness. 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. The entire regime is subject to the independent review by the Commissioner on Interception of Communications and Surveillance (the Commissioner), who would no doubt wish to review cases of multiple renewals.
11. "Also" and "Further" Authorizations	
There should not be any "*deeming provisions*".	Clauses 29 and 30 clearly set out what is authorized under a prescribed authorization, including actions which are essential for carrying out the authorized operations, and actions which are 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). 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.
12. Sanctions for Abuse	
In the recent judgment of *Watkins v. Home Office and others* [2006] UKHL 17, civil action in tort for misfeasance in public office by the victim failed, as he had suffered no "material damage", even through the public officers acted in "bad faith". To address this, the Bill should specifically provide for the creation of a statutory duty on the part of any public officer to respect privacy in general, and observe LPP in particular; any	The issue of civil remedies for invasion of privacy will be considered under a different context in the light of the LRC report on civil liability for invasion of privacy. An aggrieved individual would be able to bring an action in tort for misfeasance in public office, trespass to property or trespass to the person, depending on the circumstances of the case. He would also be able to bring an action for breach of the Hong Kong Bill of Rights Ordinance if his right under Article 10 (right to fair and public hearing), Article 11 (rights of persons charged with criminal offence) or Article 14 (protection of privacy, family, home and correspondence) of the Bill of

Issue	*Response*
breach of such statutory duty, if not in good faith, would give rise to both criminal proceedings and a civil remedy in damages against that public officer by the individuals whose rights have been infringed, without the necessity of proof of "material damage". Offences should be created for "deliberate" or "reckless" (i) unauthorized covert surveillance; and (ii) dealing with protected products in an improper manner (e.g. disclosure of protected products to third parties). LEAs have significant resources and intrusion by LEAs would not be on the same scale as individuals. Intrusions into privacy are so great that LEAs should be criminally sanctioned for any abuse, and it should not be left to internal disciplinary action as put forward by the Administration.	Rights has been violated by a LEA. While no criminal sanctions are provided under the Bill, there are existing offences (such as misconduct in public office) which may be applicable. Such offence need not be related to whether the person is liable civilly. The Commissioner under the Bill would also have the power to award compensation in appropriate circumstances. In recognition of the fact that a victim may suffer no material damage, the Bill expressly provides in clause 43(4) that any compensation awarded by the Commissioner may include compensation for injury to feelings. Moreover, the immunity provided under clause 61 of the Bill is a limited one, as LEA officers acting in bad faith would not be protected by the clause. Nor would the LEAs be immune from liability for trespass under that clause. We consider that the existing regime already strictly regulates LEA officers in conducting covert operations, and provides sufficient safeguards against abuse.
13. Notification given to data subjects	
An intercepted target should be notified of the covert operation unless it will jeopardize the operation or investigation. Sufficient details should also be provided to enable the target to decide whether or not he should seek compensation. The target should also be allowed access to the application documents (save and except those sensitive parts	The grounds against a general notification mechanism are already 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*
where the LEAs can legitimately claim public interest immunity).	
14. Data access request rights of data subject	
Clause 45(2) which grants outright denial of access of personal data is unnecessary.	As explained in our earlier response to this point raised by the Privacy Commissioner, due to the sensitive nature of the details involved in such covert operations, it is not appropriate to allow the applicant to access the relevant information. The provisions in question are aimed to protect the Commissioner on Interception of Communications and Surveillance from such demands of the applicant.
15. The Commissioner on Interception of Communications and Surveillance	
The Commissioner should be a retired High Court Judge or above. The Commissioner should have the authority to investigate whether the original authorization was validly granted, and should not be constrained in his examination functions by the principles applicable to judicial review (JR). The Report to the Chief Executive (CE) should be comprehensive and the provisions in the Bill, as drafted, are inadequate.	As explained in our response to the earlier submissions, 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 and former Permanent Judges of the CFA to be eligible for appointment as the Commissioner. As a matter of legal policy, coercive orders should not be liable to appeal. The test of JR 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 the same as that applied by the United Kingdom (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. The list of information to be provided in the Commissioner's annual report to the

Issue	*Response*
	CE is already very comprehensive, and is comparable to, if not more than, that given in overseas jurisdictions.
16. Effective Remedies	
There should be a positive duty to notify as soon as it does not compromise the investigation, and the remedies should be in line with the recommendations of the Law Reform Commission. There should be provisions in the Bill providing for a right of appeal to the Court of Appeal and the relevant procedures, to enable such a right to be pursued.	Our response to the need for notification of the target is set out under Issue 13 above. Without any overriding provisions, the Commissioner's action will be subject to judicial review. There is no need for an explicit provision on this regard.
17. Code of Practice	
The Code of Practice must be introduced as subsidiary legislation.	Clause 59 provides that the code should be made by the Secretary for Security. The code seeks to provide practical guidance to LEAs on the basis of the principles and requirements set out in the Bill. And as we have informed the Security Panel and the Bills Committee previously, the Code will be published. The present arrangement under the Bill is therefore considered appropriate.
18. Disclosure	
The defence in criminal proceedings should have access to the intercepted materials and be able to produce them as evidence solely for the purpose	We have elaborated on the proposed regime of evidential use of intercepted materials in Annex A12 to the Bills Committee paper SB Ref: ICSB 1/06. The present provisions follow the UK practice in this regard. Specifically, the UK

Issue	*Response*
of the defence. In addition, there should be a duty to retain all unused materials until the conclusion of all proceedings including appeals.	practice has been held to be consistent with the principle of "equality of arms" since neither the prosecution nor the defence has 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.

Security Bureau
June 2006