INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE BILL

COMMENTS OF THE HONG KONG BAR ASSOCIATION

Executive Summary

1. The Hong Kong Bar Association ("the Bar") considers that legislation to regulate interception of communications and covert surveillance by government actors must be demonstrably consistent with the guarantees of fundamental rights and freedoms under Chapter 3 of the Basic Law of the HKSAR, and the International Covenant on Civil and Political Rights ("ICCPR"). The drafting in the legislation must also be unambiguous, drawn narrowly and with precision.

2. The Bar is of the view that the subject matter of the Bill really warrants more time being devoted to exploring legislative options.

3. The Bar is of the view that the Bill, as presently drafted, does not provide for a regulatory scheme for interception of communications and covert surveillance by public officers that is consistent with the guarantees fundamental rights and freedoms under Chapter 3 of the Basic Law and the ICCPR. Substantial amendments are required to refine definitions, introduce adequate safeguards and remove constitutional anomalies.

<u>Who does the Bill Bind?</u>

4. The Bill binds only "public officers": see Clauses 4 and 5. It does not contain a definition of "public officer". The definition of "public officer" in the Interpretation and General Clauses Ordinance (Cap 1) section 3, which applies generally, seems to exclude persons not holding an office with the Government of the HKSAR but nonetheless acting on its behalf. This problem ought to be addressed, as the regulatory regime prescribed in

the Bill can readily be evaded by relying on "privatising" intelligence gathering to non-descript individuals.

Interception of Communications

5. The Administration should clarify whether it proposes to classify the monitoring and recording of data transmitted under broadband (wireline and wireless) telecommunications services to be an "intercepting act" and thus coming under the regulatory scheme for interceptions of communications instead of the scheme for covert surveillance.

6. The Administration should also clarify whether it proposes to classify the monitoring and recording of voice and data (such as SMS and e-mails) transmitted between a mobile telephone/personal data assistant and the corresponding cellular telecommunications transmitter to be an "intercepting act" and thus coming under the regulatory scheme for interceptions of communications instead of the scheme for covert surveillance.

7. The Administration should explain why it is envisaged in paragraph (b) of the definition of "interception" that a prescribed authorization under the Bill for interception of communications may be in such broad terms as to be without any specific reference to the communication(s) that will be inspected (including listened to, monitored and recorded) by a third party.

8. The Administration's proposal in Schedule 5, paragraph 5 of the Bill to substitute section 33 of the Telecommunications Ordinance (Cap 106) with a new provision to empower the Chief Executive to order "*any class of messages to be intercepted*" for the facilitation of the detection or discovery of offences under that Ordinance, and the execution of prescribed authorizations for telecommunications interception is alarming. This provision appears to provide for a broad power, to be exercised solely by the Chief Executive, for wholesale, routine and continuous monitoring and recording of telecommunications (including voice and data

transmissions), without any mechanism for outside authorization and oversight. The Administration should explain what it considers to be: (1) "facilities reasonably required for the execution of prescribed authorizations for telecommunications interception" and (2) the classes of "messages" sought to be intercepted pursuant to each of the proposed section 33(1)(a) and (b). The Administration should justify with cogent reasons this proposal and amend it to ensure that any such power (if it were ever justified for a legitimate purpose) must be subject to proper authorization and oversight and must not be used to circumvent the main provisions of the Bill.

Covert Surveillance: Type 2, paragraph (a) surveillance

9. The definition of "covert surveillance" includes forms of surveillance which could result in the recording of conversations. However, the definition of "Type 2 surveillance" means that if surveillance with a device recording conversation covertly is carried out by a person participating in the conversation, such surveillance (or Type 2, paragraph (a) surveillance), albeit done covertly, does not require judicial authorization.

10. Type 2, paragraph (a) surveillance also includes forms of surveillance which could reproduce documents in the permanent form. The definition of "data surveillance device" is wide enough to include physical devices and computer "viruses" that monitor or record any stream of data that goes and out of computer or data processing systems, including e-mails, file transfers/copying, and key strokes. The definition of "information system" is wide enough to include, when used in conjunction with that of "data surveillance device", as covert surveillance all monitoring or recording of data input and output in relation to a computer, a personal data assistant, or a mobile telephone, subject only to the exception in paragraph (b) of the definition of "covert surveillance" in respect of "*systematic surveillance to the extent that it constitutes interception under [the Bill]*".

11. Covert surveillance that results in the making of a permanent record of what was done and/or said and/or typewritten may interfere with a person's "reasonable expectation of privacy" as much as the interception of their communications, such as a telephone call. It makes no difference whether A is sending a letter to B or e-mailing B or telephoning B or speaking to B, face to face. They are simply different forms of communication.

12. The Administration should provide satisfactory justification for the difference in treatment in terms of the authority for authorization between Type 1 surveillance and Type 2, paragraph (a) surveillance.

Covert Surveillance: Type 2, paragraph (b) surveillance

13. The definition of "Type 2 surveillance" includes in paragraph (b) the use of a tracking device which does not involve: (i) the entry into premises without permission, or (ii) the interference with the interior of any conveyance or object without permission. Therefore, under (i) it would include the attachment of a listening device to the outside of premises which could be equally effective. Under (ii) it would cover the attachment of a tracking device to the outside of a vehicle. Therefore, by just installing the tracking device to the exterior (and underside) of a vehicle the investigator will not require any outside authorization, yet obtain the information needed, with minimal risk of discovery.

Covert Surveillance: "Entitled to" reasonable expectation of privacy

14. Paragraph (a)(i) of the definition of "covert surveillance" states that systematic surveillance is qualifying surveillance if it is carried out in circumstances where the target person is "*entitled to a reasonable expectation of privacy*". This manner of drafting is infelicitous and risks the protective mechanism of the provisions of the Bill being circumvented as a result of a junior investigating officer's own unskilled and subjective perception about another person's reasonable expectation of privacy.

Covert Surveillance: Activities in public places

15. Clause 2(2) seeks to modify a person's reasonable expectation of privacy to the extent that he is not entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place. The definition of "public place" in Clause 2(1) is all-inclusive and excludes only public toilets or bathing or changing facilities. Therefore, clause 2(2) seems to hold that one's conversation on the mobile phone on the street or with a friend in a restaurant may be subject to surveillance and audio recording by public officers covertly without any requirement for authorization of any kind.

16. The Bar considers that Clause 2(2) is based upon an erroneous understanding of the right to privacy and violates Article 39 of the Basic Law and Article 17(2) of the ICCPR (right to privacy). A person has a "reasonable expectation of privacy" even in a public place.

17. Legislation cannot limit the right to privacy guaranteed by the Basic Law and the ICCPR. *Basic Law rights and freedoms are neither dependent upon nor defeasible by ordinary law.* Clause 2(2) is an overt attempt of the Administration to overturn unfavourable and inconvenient jurisprudence. It is an impermissible move asking the legislature to usurp the judicial prerogative of interpretation of the Basic Law. It should be deleted.

Conditions for Prescribed Authorization: Serious crime

18. The Bill prescribes as a legitimate purpose for obtaining a prescribed authorization the purpose of prevention or detection of "*serious crime*": Clause 3(1)(a)(i). That expression is defined in Clause 2(1) to include, in respect of the interception of communications, offences punishable by over 7 years' imprisonment. In effect that would include all indictable offences. For covert surveillance, it covers offences punishable by 3 years'

imprisonment. That would take in all indictable offences, and many summary offences.

19. The scope of the definition of "serious crime" in the Bill is far too broad. The Bill should cover only the most serious offences so that the interference with privacy is proportional.

20. The Administration should explain why "serious crime" under the Bill is not defined by way of enumerated lists of offences, described by reference to the conduct involved, or common feature(s) in the conduct involved.

Conditions for Prescribed Authorization: Public Security

21. The Administration has not indicated which of the law enforcement agencies proposed to be included in Schedule 1 of the Bill has the duty to "protect public security". None of them has an express statutory duty to "protect public security".

22. The Bill incorporates the protection of "public security" as a legitimate purpose for obtaining a prescribed authorization presumably because of the language of Article 30 of the Basic Law, i.e. "public security" (gonggonganquan). The fact that Article 30 of the Basic Law mentions that expression is not necessarily a good and sufficient reason for incorporation. The wording of Article 30 of the Basic Law follows closely with that of Article 40 of the Constitution of the People's Republic of China, but the corresponding term of "public security" (gonggonganquan) in Article 40 is "state security" (guojiaanquan). A study of Mainland law indicates that "public security" (gonggonganquan) is a concept distinct from that of "state security" (guojiaanquan).

23. Given that –

- the Bill is not intended to regulate activities taken by or on behalf of the Central Authorities or its subordinate organs in Hong Kong;
- the statutory duties of the law enforcement agencies proposed to be included in Schedule 1 of the Bill do not appear to express a duty to protect "public security" (gonggonanquan);
- conduct that truly endangers "public security" (gonggonanquan) is arguably criminal conduct punishable by such substantial term of imprisonment and of such reprehensibility as to qualify as a serious crime; and
- the Administration does not wish to narrowly define "public security" (gonggonganquan) in the Bill,

it is advisable to leave out of the Bill the concept of "public security" (gonggonanquan).

Conditions for Prescribed Authorization: Threshold for findings

24. Clause 3 does not prescribe any threshold that a panel judge or authorizing officer of a department must be satisfied on matters of fact before a prescribed authorization is issued.

Conditions for Prescribed Authorization: Proportionality test: Balancing, in operational terms, relevant factors

25. The test of proportionality prescribed in Clause 3(1)(b) may be difficult to administer. The requirement to undertake a "balancing" of "relevant factors" in making a determination under the Bill may result in decision-makers, particularly those not legally trained, unconsciously lapsing into an exercise of personal value judgments. This may lead to a lack of uniformity in approach. The Commissioner on Interception of Communications and Surveillance ("the Commissioner") does not appear to be in a position to have a complete overview of all the activities provided for under the Bill to serve as a source of guidance.

26. The Administration should explain the need to insert into the test of proportionality test the qualifying term of "in operational terms".

Legal Professional Privilege

27. Lawyers and the public must be assured that the communications between lawyers and their clients will be privileged and not recorded and examined.

28. The Bill, however, envisages that interception of communications and covert surveillance may be carried out against lawyers. The Administration should justify why it does not exclude legal professional privileged communications from being the object of activities authorized under it.

29. Clause 2(3) leaves it to the public officer to determine whether it is likely that legal professional privileged communications will be obtained in the course of surveillance. That is not an adequate protection. There is no threshold requirement that the applicant must show, or that the panel judge or senior law enforcement officer must be satisfied of, before granting an authorization that may record such communications. The requirement in Schedule 3, Parts 1 to 3 for a statement in the affidavit in support of likelihood of legal professional privileged information to be obtained is not detailed enough. All safeguards must be taken so as to ensure that no legal professional privileged communications are recorded.

30. The Administration should amend the Bill to provide that where any proposed interception of communications or covert surveillance might involve a barrister, solicitor, solicitors clerk or legal executive, whether by reference to circumstances, location or parties, there needs to be obtained a prior judicial authorization, given only after strict scrutiny in accordance with a high threshold of justification. No emergency applications may be made in this connection.

31. Even where an authorization is issued to intercept or conduct surveillance of communications that might be the subject of legal professional

privilege, the Bill must require conditions to be imposed against the authorization to "avoid so far as practicable the [inspection, listening to, monitoring or recording] of communications of a professional character" to which the lawyer or his employee, pupil, trainee, intern or associate may be a party.

32. The Administration should amend the Bill to preserve the character of legal professional privileged communications captured as the product of an interception of communications or surveillance under a prescribed authorization. Such product should remain inadmissible as evidence before any court without the consent of the person entitled to waive the privilege.

33. The Administration should amend the Bill to make provision for the immediate destruction or turning over to a panel judge for retention and ultimate disposition of such product of an interception of communications or surveillance pursuant to a prescribed authorization that unintentionally or unexpectedly captures communications under legal professional privilege.

34. The Administration should amend the Bill to require law enforcement agencies to notify all lawyers whose chambers, office, or residence; or whose person, or whose pupil, trainee, staff, intern or associate, has been the object of an interception of communications or surveillance pursuant to a prescribed authorization of the particulars of the interception or surveillance, including but not restricted to, particulars of time and duration of interception or surveillance, the methods used, and the communications inspected, listened to, monitored and/or recorded.

Criminal Sanctions

35. Non-compliance with any of the substantive provisions of the Bill should be a criminal offence.

"Judicial Authorization" by Judges of the Court of First Instance

36. The proposed scheme of authorization by panel judges for interception of communications and Type 1 surveillance is one of executive authorization by judges.

37. There are legal policy objections to having judges of the Court of First Instance as panel judges. They are:

(a) Schedule 2, paragraph 4 of the Bill seems to suggest that decisions of panel judges under the Bill are amenable to judicial review by the Court of First Instance. Where an "administrative decision" of a judge of the Court of First Instance that is amenable to judicial review is the subject of an application for judicial review, the practice is for two other judges of the Court of First Instance to hear the application. That problem would not arise if some other authority was chosen.

(b) Panel judges will be "conflicted out" of any criminal trial or appeal where the prosecution has sought an authorization from him or her.

38. These legal policy objections need to be answered in the context of the question: "*What is the rationale for not appointing District Court Judges to do this work?*" There are more District Court judges and so the opportunities for avoiding conflict are greater.

39. The Administration must assure the public that the new legislation will not impair the operational efficiency of the Judiciary and the law enforcement agencies.

40. Schedule 2, paragraph 4 of the Bill should be re-positioned to the body of the Bill.

41. The drafting of Clause 6 and Schedule 2, paragraph 4 of the Bill must indicate clearly that it is intended that individual judges detached from the

court they constitute are being vested with a non-judicial power. As presently drafted, these provisions of the Bill fail to indicate uncontrovertibly that the proposed conferral of power upon the panel judges is to be consented to by each and every one of them. Further, the inclusion of the expression of "shall act judicially" in Schedule 2, paragraph 4 may give rise to confusion about the true nature of the power to be conferred.

42. The Administration must bear in mind that the proposed conferral of power on panel judges to authorize interception of communications and Type 1 surveillance under the Bill implies a continuing constitutional obligation to ensure that the performance of statutory functions under the Bill will not become incompatible with the institutional integrity of the Judiciary and the individual integrity of its members.

43. The Administration has indicated that it will require panel judges to be subject to "extended checking" before appointment, "as they will have access to highly sensitive materials". It should be noted that all judges and judicial officers may in the course of their careers encounter cases involving public interest immunity claims and have to rule on the validity of such claims by considering privately such documents. The present arrangement of "appointment checking" must have been put in place against this background. The Administration has <u>not</u> put forward a case to justify the imposition of the highest level of integrity checking upon panel judges candidates.

<u>Applying for a Judicial Authorization</u>

44. The Administration should explain why it proposes applications for judicial authorization should not be vetted by the Department of Justice and made by counsel of that department. Approval by a directorate officer of the relevant department does not appear to be an adequate safeguard.

45. Schedule 3 of the Bill does not require a public officer making an application for a judicial authorization to state that he has "reasonable grounds to believe" that an offence has been or is about to be committed or that there is a threat to public security. The schedule requires him to merely state why the purpose sought to be furthered by carrying out the interception of communications or Type 1 surveillance cannot reasonably be furthered by other less intrusive means.

46. Corresponding provisions in Canada, New Zealand and the United States, require the law enforcement agency to try other investigative means before resorting to the interception of private communications. Even Hong Kong's Organized and Serious Crimes Ordinance (Cap 455) section 3 and Interpretation and General Clauses Ordinance section 84(3) incorporate more stringent conditions to be fulfilled than Schedule 3, Part 1 or Part 2 of the Bill.

47. Panel judges rely on the information provided in the affidavit to make determinations on whether an authorization should be issued. Panel judges are not spymasters by training. They are not in a position to cross-check the information provided unilaterally by the applicant, or to argue with or investigate the truth of the facts asserted. Therefore, the information and fact sought to be asserted before the panel judge must be fully particularized and meet a high threshold of assurance. The Administration should explain the above inadequacies and inconsistencies in Schedule 3, Part 1 or Part 2 of the Bill.

Determining an Application for Judicial Authorization

48. It is necessary for the Bill to contain provisions requiring the panel judge to consider and formulate the terms of his authorization to minimize the interference with the right to privacy.

Duration and Renewal of Judicial Authorization

49. The Administration must justify the 3 month period of authorization proposed in the Bill.

50. There is no limitation in the Bill in the number of renewals or in the maximum number of days in which an authorization may last, so long as "*the conditions for its grant under section 3 have been met*": Clause 12. The information proposed to be set out in an affidavit in support of an application for renewal does not appear to provide the full extent of information relevant to the assessment by a panel judge. The Bill should be amended to introduce provisions that require a panel judge, in considering an application for renewal, to take account of the aggregate length of interception of communications or surveillance undertaken, and to oblige the applicant to provide greater justification for renewal of authority where a long period of interception or surveillance has already taken place.

Executive Authorizations

51. The Bar's views on the contents of the affidavit to be prepared for an application for a judicial authorization, on the specifying conditions in a judicial authorization and the duration of an authorization or its renewal above applies equally to executive authorizations.

52. The Administration should explain why it proposes applications for renewals of an executive authorization should remain internal within the same department and not to be before a panel judge or some outside party for consideration.

"Also" and "Further" Authorizations

53. Clauses 29(6) and (7) provide for activities that a prescribed authorization for interception or covert surveillance "also authorize". Contrast with the

provisions in Clauses 29(1) to (5), which provides that a prescribed authorization "may contain terms that …". The Administration should explain why it does not draft Clauses 29(6) and (7) in the way Clauses 29(1) to (5) are drafted.

54. Clause 30 provides in general terms that a prescribed authorization "*further authorizes 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*". The terms of this proposed statutory "further authorization" are very broad and might arguably be applied to cover arbitrary activities. Such formulation of the generality portion of this clause is most inappropriate.

55. Clause 30 also lists a number of activities that is sought to be "further authorized", The Administration should explain why it does not draft Clause 30(c), (d) and (e) in the way Clauses 29(1) to (5) are drafted so that the activities covered in Clause 30(c), (d) and (e) are only authorized upon the conscious decision of the relevant authority.

<u>Emergency Applications</u>

56. The Administration should justify its refusal to entrust emergency applications to panel judges, bearing in mind that applications may be made orally.

57. The criteria for emergency authorizations are set out in Clause 20(1)(a), and includes under (iv), "*loss of vital evidence*". This criterion seems too broad a category to allow for emergency authorizations for interceptions of communications or Type 1 surveillance to be made by the head of a department.

Notification

58. A person who has been the object of an authorization or in general terms, has had his privacy interfered with, must be informed of this so that he can decide to pursue whatever remedy is available.

Civil Immunity

59. In general, civil liability for unlawful activities carried out in contravention of the Bill will act as a deterrent against abuse.

60. The immunity provisions in Clause 61 appear to be too wide. Only Clause 61(1)(a) alone is acceptable.

The Commissioner on Interception of Communications and Surveillance

61. To avoid the appearance of a serving judge reviewing the performance of other serving judges, the appointment of the Commissioner should be an appointment made of a former judge under Clause 38(6)(c)-(e). Such an appointment would not be a drain on judicial manpower resources.

62. Clause 53 shows that the Administration's proposal is that in so far as a serving judge under Clause 38(6)(a)-(b) is sought to be appointed as the Commissioner, he is to be appointed as an individual judge detached from the court he constitutes. The Bar's comments above on the constitutional position of panel judges apply equally to a Commissioner whose eligibility derives from his current service as a judge. Clause 38 should as a result be suitably amended.

63. Clause 42(1) provides that if a person "*believes*" that his communications have been intercepted or he has been the object of covert surveillance carried out by a department, he may apply to the Commissioner for an examination. Such a formulation is problematic. A threshold of "*suspects*" would be more appropriate.

64. Clauses 43(1)(b) and (2) appears to contain a drafting error. A better drafting should refer to "a prescribed authorization should have been, but has not been, *applied for* or renewed under this Ordinance".

65. The Commissioner should not be constrained in his examination functions by the straitjacket of "principles applicable to judicial review": Clause 45(1)(a).

66. The Commissioner is to make a report to the Chief Executive pursuant to Clause 47. The requirements as to the content of the report are too limited. The report should contain comprehensive information that the Chief Executive and the Legislative Council require in order to see if the law is being abused or is effective. The contents of similar reports in overseas jurisdictions give far more information, and should be looked at as models.

Effective Remedies

67. It is doubtful whether a HKSAR resident whose activities have been subject to unlawful interception of communications or covert surveillance by public officers can have effective remedies against such abuse of power. The covert nature of the interception or surveillance conducted against the resident would make it difficult for him to discover the fact of action taken against his reasonable expectation to privacy. He cannot begin the process of seeking remedies on the basis of a suspicion of interception or surveillance.

Code of Practice

68. The Code of Practice should be laid before the Legislative Council and should address similar issues to those addressed in the codes of practice in the United Kingdom so that the public know the circumstances when there may be interference with their right to privacy under the law and the

yardstick which the Commissioner measures the performance of law enforcement agencies under the legislation.

Disclosure

69. There is a strong body of opinion among experienced members of the Bar practising in criminal law that notwithstanding the intention of the Administration not to have any telecommunications interception product admissible in any proceedings before any court, the defence in criminal proceedings should have access to it, and, be able to produce it as evidence for the purpose of demonstrating innocence. The right to a fair trial is a fundamental right guaranteed under the Basic Law and the ICCPR, and a common law right that the courts will safeguard jealously. The right to material disclosure is an aspect of fair trial.

70. Clause 58(4) as presently formulated, seriously limits the prosecution's duty of disclosure under common law.

71. Clause 58(6) has 3 problems. Firstly, the judge has the power to direct the prosecutor how to conduct the case, i.e. to make an admission of fact. Secondly, and more importantly, the judge has no power to order the disclosure of the "products" of the interception.

72. The third problem is fundamental to the interests of the defence. The admission of fact is disclosure only of information from the telecommunications interception product, and not the product itself. The information is invariably compiled by senior officers of the law enforcement agency involved in the particular case. Given that the process by which the information is compiled cannot be questioned or probed into at trial because of Clause 58(3), the defence cannot begin to procure admission of additional information.

73. Clause 58(3) prohibits the asking of any questions about a prescribed authorization for interception of communications and constitutes a

significant retrograde step from the present practice, which permits inquiry into all of the matters included in the clause as part of the criminal trial process. It denies "equality of arms". It can be seriously argued that such restrictions infringe a person's right to a fair trial, and the right to an "effective remedy".

74. The Administration must explain how it sees that the admission of the product of a prescribed authorization, and the product derived from further investigation relying on information obtained under the authorized activities, can be effectively challenged in a trial. The Administration must also explain what powers a trial judge has to exclude the evidence obtained from any authorizations.

Transitional Arrangements

75. Clause 65 of the Bill seeks to apply Clauses 56 and 58 to materials obtained by telecommunications interception under an order made pursuant to section 33 of the Telecommunications Ordinance prior to the commencement date. The proposed application of Clause 58 to such materials is inappropriate.

Consequential Amendments

76. Schedule 5 of the Bill contains consequential amendments. The proposed consequential amendment to the Personal Data (Privacy) Ordinance (Cap 486) cannot be accepted.

Dated 24th March 2006.

Hong Kong Bar Association