# 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.

Who does the Bill Bind?

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

# INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE BILL

## COMMENTS OF THE HONG KONG BAR ASSOCIATION

Object

1. The Hong Kong Bar Association ("the Bar") submits its comments of the Interception of Communications and Surveillance Bill ("the Bill"). The Bar has studied the Bill, the regulatory systems on interception of communications and covert surveillance adopted by overseas jurisdictions, and local and international jurisprudence; and consulted its membership on a list of issues, before formulating these comments.

2. The Bar aims to indicate in these Comments the problems and defects of the Bill in its gazetted draft, as well as matters that deserve further explanation or clarification from the Administration.

3. The Bar does not consider these Comments to be exhaustive. If the Bar has not commented in these Comments on any issue or matter connected with the Bill or the legislative framework proposed by the Administration to regulate interception of communications and covert surveillance by public officers, this is not to be construed to mean that the Bar agrees to, or has no objection to, or take a neutral stance on, or has no opinion on, that issue or matter.

General Observations

4. The Bar considers that the legal necessity and the community's consensus of the desirability for legislation to regulate interception of communications and covert surveillance by government actors can only be met by legislation that is demonstrably consistent with the guarantees of

fundamental rights and freedoms under Chapter 3 of the Basic Law of the HKSAR, and, by virtue of Article 39 of the Basic Law, the International Covenant on Civil and Political Rights ("ICCPR"). The drafting in the legislation must also be unambiguous, drawn narrowly and with precision.

5. The Bar notes that while the gazettal of the Bill indicates that the Administration is at long last tackling with the legal and human rights issue of the proper regulation of interception of communications and covert surveillance by government actors, the Administration had in fact waited until its hand was forced by adverse court judgements which had been long threatened. The present unseemly rush to legislate to meet a "court imposed deadline" could have been avoided had the Administration sought to implement the 1996 report of the Law Reform Commission on Interception of Communications.

6. The Bar is of the view that the subject matter of the Bill really warrants more time being devoted to exploring legislative options. The Administration should not be surprised should the Bill, if enacted in its present form, turn out to be a source of problems and legal challenges.

7. The need for rigourous scrutiny is borne out by the words of Lord Denning MR, commenting on the statutory power of search and seizure of the Inland Revenue Commissioners in R v Inland Revenue Commissioners ex p Rossminster [1980] AC 952 at 972A-C:

*The trouble is that the legislation is drawn so widely that in some hands it might be an instrument of oppression. It may be said that "honest people need not fear: that it will never be used against them: that tax inspectors can be trusted, only to use it in the case of the big, bad frauds." This is an attractive argument, but I would reject it. Once great power is granted, there is a danger of it being abused. Rather than risk such abuse, it is, as I see it, the duty of the courts so to construe the statute as to see that it encroaches as little as possible upon the liberties of the people of England.*

8. 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 of the HKSAR and the ICCPR. Substantial amendments are required to refine definitions, introduce adequate safeguards, and remove constitutional anomalies.

9. The language used in the text of the Bill suggests that the Administration has formulated its architecture by reference to the regulatory schemes in Australia and the United Kingdom. The Bar notes that Australia does not have any form of a bill of rights and the operation of the Human Rights Act 1998 of the United Kingdom since 2000 has not yet allowed that jurisdiction to fully develop a robust human rights jurisprudence in the absence of a margin of discretion that pervaded the jurisprudence of the European Court of Human Rights.

10. Whilst the regulatory scheme proposed under the Bill should be justified by examining its compliance with the human rights standards applicable to the HKSAR, as opposed to by reference to the overseas regulatory schemes on which it is based, the Bar will in the discussion below draw attention to the regulatory schemes of a number of overseas jurisdictions that guarantee protection of human rights under a written constitution or a charter or bill of rights. Particular mention will be made of the regulatory scheme in Canada under its Criminal Code, Part VI, being one that has had to be fashioned with necessary safeguards to achieve compliance with the Canadian Charter of Rights and Freedoms 1982, an entrenched constitutional instrument interpreted robustly by the Supreme Court of Canada. The Canadian scheme provides at least a workable example for Hong Kong, a jurisdiction with its constitutional instrument requiring legislation to be consistent to guarantees of fundamental rights, to seriously consider.

List of Issues

11. The Bar consulted its membership on 20 issues. The list of issues is attached herewith in Appendix A.

Who does the Bill Bind?

12. The Bill binds only "public officers": see Clauses 4 and 5. Interceptions by third parties are not covered.

13. The Bill does not contain a definition of "public officer". The definition of "public officer" in the Interpretation and General Clauses Ordinance section 3 applies: "*any person holding an office of emolument under the Government, whether such office be permanent or temporary*". "Government", in the circumstances, is taken to mean what is defined also in section 3, namely "*the Government of the HKSAR*" and thus the executive authorities of the HKSAR by virtue of the Basic Law of the HKSAR, Article 59.

14. Interceptions of telecommunications by way of interference with a telecommunications installation by "any person" are prohibited under the Telecommunications Ordinance (Cap 106) section 27(b). Section 3 of that Ordinance provides that, save as otherwise expressly provided, it does not bind "the Crown" or apply to any means of telecommunications established or maintained by "the Crown" or to any apparatus for telecommunications possessed or used by "the Crown" for the purpose of or in connection with any such means of telecommunications. The expression "the Crown" in the premises arguably makes reference to both the Central People's Government or other competent authorities of the People's Republic of China, and the Government of the HKSAR; see Interpretation and General Clauses Ordinance Schedule 8, paragraphs 1 and 2. There is no express provision to the contrary intent of section 3 of the Telecommunications Ordinance in respect of section 27(b) of the same.

15. Although the Bill does not contain a provision specifying that its provisions shall bind the State, as defined under section 3 of the Interpretation and General Clauses Ordinance, it binds, as a matter of necessary implication, the part of the definition of the State known as the Government of the HKSAR. The Administration appears to agree that section 66 of that Ordinance applies and the Bill does not affect the right of or be binding on, for example, the Central People's Government and any of its subordinate organs that, on its behalf, exercises executive functions of the Central People's Government or functions the Central People's Government has responsibility under the Basic Law of the HKSAR, and do not exercise commercial functions, when acting within the scope of the delegated authority and the delegated functions of the subordinate organ concerned. See the Legislative Council Brief of the Security Bureau (March 2006) paragraph 17 and the Legislative Council Paper on Response to issues raised by Members at the meeting of 7 February 2006 of the Security Bureau (February 2006) paragraph 4.

16. The Administration may wish to assure the public that interception of communications and covert surveillance will not be carried out by office-holders of or on behalf of the State who are not public officers within the meaning of the Interpretation and General Clauses Ordinance. The Administration may also wish to indicate whether it proposes to address this problem and if so, by what means.

17. Apart from the problem relating to persons holding an office or acting on behalf of the Central Authorities or a subordinate organ thereof, the definition of "public officer" itself seems to exclude persons not holding an office with the Government 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.

18. The Administration has indicated that it will address the problems of non-government actors later. The Administration should indicate how "temporary" this temporary arrangement is.

Interception of Communications

19. The definition of "interception" in Clause 2(1) contains two alternative paragraphs:

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

20. Paragraph (b) suggests that a prescribed authorization under the Bill may be issued without any specific reference to the communication(s) that will be inspected (including listened to, monitored and recorded) by a third party. See Clause 29(1), which proposes to permit prescribed authorizations to be made in terms that specify only the premises, address or object person.

21. The Administration should explain why it is proposed that a prescribed authorization under the Bill for interception of communications may contain such broad terms.

22. The definition of "intercepting act" in Clause 2(1) seems to cover the inspection (including listening, monitoring and recording) of telecommunications in the course of its transmission by both wireline and wireless telecommunications systems.

23. 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 regulatory scheme for covert surveillance.

24. 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 cum 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 regulatory scheme for covert surveillance.

25. The Administration proposes in Schedule 5 of the Bill, paragraph 5 to substitute section 33 of the Telecommunications Ordinance with a provision (i.e. the proposed section 33(1)) to empower the Chief Executive to order "*any class of messages to be intercepted*" for "*the purpose of providing or making available facilities reasonably required for –*

*(a) the detection or discovery of any telecommunications service provided in contravention of any provision of [the Telecommunications Ordinance] or any regulation made under [the Telecommunications Ordinance] or any of the terms or conditions of a licence granted under [the Telecommunications Ordinance]; or*

*(b) the execution of prescribed authorizations for telecommunications interception that may from time to time be issued or renewed under [the Bill]*."

This provision appears to provide for a broad power for wholesale, routine and continuous monitoring and recording of telecommunications (including voice and data transmissions), albeit not on an individualized basis (see the proposed section 33(2)), so that such records of telecommunications may subsequently be accessed whenever a prescribed authorization is issued and sought to be executed.

26. The proposed section 33 of the Telecommunications Ordinance is alarming. The Chief Executive alone is sought to be given the power to make orders putting unspecified class(es) of telecommunications to be under presumably routine and continuous monitoring and recording if he considers it "*reasonably required*" for facilitating the operation of the Bill. Such orders are not required under the proposal to be published. The Commissioner on Interception of Communications and Surveillance ("the Commissioner") under the Bill has no jurisdiction over the Chief Executive's orders. See Clause 39. No provision is proposed to provide for the regulation of the storage, use and disclosure of telecommunications messages intercepted pursuant to a Chief Executive's order. There is no consequential amendment to the Personal Data (Privacy) Ordinance (Cap 486) dealing with the data collection exercises under the proposed provision.

27. Although Clause 10(a) appears to provide a safeguard that an authorization for interception of telecommunications is not to take effect earlier than the time when the authorization is issued, the perceived prospective operation of the authorization is illusory if the proposed section 33 of the Telecommunications Ordinance is capable of being applied to intercept classes of telecommunications from time to time and to keep as "stored communications" to be accessed as soon as there is an authorization with a specified object by reference to address, premises or person. The proposed section 33(2) might be capable of preventing this form of abuse of power. 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).

28. The Administration should justify with cogent reasons the proposal to substitute section 33 of the Telecommunications Ordinance with the proposed provisions. The Administration should amend the proposal to ensure that any power to intercept telecommunications generally and for a facilitating purpose (if it were ever justified as a legitimate purpose) must

be subject to proper authorization and oversight and must not be used to circumvent the main provisions of the Bill for case-by-case and independent and impartial authorization of interception of telecommunications.

Covert Surveillance: Type 2, paragraph (a) surveillance

29. The definition of "covert surveillance" in Clause 2(1) includes forms of surveillance which could result in the recording of conversations. However, the definition of "Type 2 surveillance" in Clause 2(1) 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.

30. Type 2, paragraph (a) surveillance also includes forms of surveillance which could reproduce documents in the permanent form. The definition of "data surveillance device" in Clause 2(1) is wide enough to include physical devices and computer programmes (better known as "viruses" and "Trojan Horses") 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" in Clause 2(1) 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 Clause 2(1) in respect of "*systematic surveillance to the extent that it constitutes interception under [the Bill]*". Accordingly, systematic surveillance of data exchanged between terminals in a closed data network of a company is covert surveillance within the meaning of the Bill and comes within Type 2, paragraph (a) surveillance if done by a person capable of accessing the network using a data surveillance device.

31. 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. It can in fact be strongly argued that the more transient the form of communication (i.e. leaving no permanent record, unlike letter or e-mail), the greater and thus more reasonable the expectation that there will be no interception, intrusion, recording using a device by outsiders etc. as nothing is normally expected to be produced or reproduced to be read or heard by someone else.

32. The aspect of video surveillance and constitutional rights was addressed by the Supreme Court of Canada in R v Wong (1991) 60 CCC (3d) 460. In that case the Court discussed the issue of visual/optical surveillance where the police had installed a video camera in a hotel room to monitor illegal gambling. At the time there was no statutory provision for judicial authorizations of such surveillance. The Court's discussion of "reasonable expectation of privacy" in such circumstances may serve to contrast the Administration's position. Chief Justice Lamer said at p 465E-F:

> *A person has the right, under s.8* [protection against unreasonable search and seizure] *to be free from unauthorized surreptitious electronic surveillance where that person has a reasonable expectation that the agents of the state will not be watching or recording private activity nor monitoring or recording private conversations. Whether such an expectation is reasonable will depend on the particular circumstances; a person does not necessarily enjoy this right in all circumstances.*

La Forest J discussed the Court's earlier decision in R. v. Duarte at p 478A:

> *In the place of 'risk analysis', R. v. Duarte approached the problem of determining whether a person had a reasonable expectation of privacy in*

*given circumstances by attempting to assess whether; by the standards of privacy that persons can expect to enjoy in a free and democratic society, the agents of the state were bound to conform to the requirements of the Charter when effecting the intrusion in question. This involves asking whether the persons whose privacy was intruded upon could legitimately claim that in the circumstances it should not have been open to the agents of the state to act as they did without prior judicial authorization…..the adoption of this standard invites the courts to assess whether giving their sanction to the particular form of unauthorized surveillance in question would see the amount of privacy and freedom remaining to citizens diminished to a compass inconsistent with the aims of a free and open society.*

And at p 478F-G:

*Accordingly, the standards of privacy that prevail in a free and open society such as our own, Duarte was entitled to claim that judicially unauthorized participant surveillance did offend against his reasonable expectation of privacy when he engaged in what he had every reason to believe was an ordinary private conversation. To have held otherwise would have been tantamount to exposing any member of society whom the state might choose to target to the same risk of having his or her nominally private conversation become the subject of surreptitious recordings.*

And at p 479A-F:

*I am firmly of the view that if a free and open society cannot brook the prospect that the agents of the state should, <u>in the absence of judicial authorization,</u> enjoy the right to record the words of judicial authorization, enjoy the right to record the words of whomever they choose, it is equally inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious video surveillance. George Orwell in his classic dystopian novel, 1984, paints a grim picture of a society whose citizens had every reason to expect that their every movement was subject*

*to electronic video surveillance. The contrast with the expectations of privacy in a free society such as our own could not be more striking. The notion that agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconciable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonable expect to enjoy in a free society. There are…situations and places which invite special sensitivity to the need for human privacy. Moreover, as Duarte indicates, we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.*

And at p 482H:

*Moreover, it is also clear that those ordinary measures which persons in a free and open society believe suffice to shut out uninvited scrutiny would be of no avail if the police (and they would of course be the sole arbiters of the matter) entertained the suspicion that the persons in the location concerned were invited in illegal activity.*

And at p 483D-F:

*I take it to be beyond dispute that just as we hold to the belief that a free and open society is one in which the state is not free to make unauthorized recordings of our conversations, so to it is no less an article of faith in a society that sets a premium on being left alone that its members presume that they are at liberty to go about their daily business without courting the risk that agents of the state will be surreptitiously filming their every movement…it must follow that unauthorized video surveillance will be found to offend against the reasonable expectations of privacy protected by s.8 in the circumstances here.*

33. After R v Wong (supra), the Canadian Parliament enacted section 487.01 of the Criminal Code which covers all investigative devices which do not involve the interception of private communications (which are covered in Part VI of the Criminal Code). Section 487.01 reads, in its current form, in part:

> *(1) A provincial court judge, a judge of the superior court of criminal jurisdiction…may issue a warrant in writing authorizing a peace officer to, subject to this section, use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property…*
>
> …
>
> (3) *A warrant issued under subsection (1) shall contain such terms and conditions as the judge considers advisable to ensure that any search or seizure authorized by the warrant is reasonable in the circumstances.*
>
> (4) *A warrant issued under subsection (1) that authorizes a peace officer to observe, by means of a television camera or other similar electronic device, any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy shall contain such terms and conditions as the judge considers advisable to ensure that the privacy of the person or of any other person is respected as much as possible.*

34. 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. The Administration should note that long standing operational usage of Type 2, paragraph (a) surveillance previously by law enforcement agencies does not, by itself, constitute satisfactory justification.

Covert Surveillance: Type 2, paragraph (b) surveillance

35. 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. This was the type of listening device used in R v Khan [1997] AC 558 (House of Lords) which recorded the appellant's conversations. 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 about the where the vehicle is at any time, with minimal risk of discovery. In R v Wise (1992) 70 CCC (3d) 193, a tracking device was installed in the interior of the appellant's vehicle. The majority of the Supreme Court of Canada held that the beeper monitoring of the appellant's vehicle violated a reasonable expectation of privacy [p 221E], but found that the evidence was admissible in the circumstances. La Forest J (in dissent) said at p 203C-G:

*I must confess to finding it absolutely outrageous that in a free society the police or other agents of the state should have it within their power, at their sole discretion and on the basis of mere suspicion, to attach a beeper on a person's car that permits them to follow his or her movements night and day for extended periods…*

...

*What I quarrel with is that the police or agents of the state should have the power to use electronic equipment permitting them, at their whim, to know where any particular individual may be at any time without the authorization of the judiciary or some other independent third party.*

36. After R v Wise the Canadian Parliament enacted section 492.1 of the Criminal Code which covers all tracking devices. Section 492.1 reads, in its current form, in part:

*(1)* *A justice who is satisfied by information on oath in writing that there are reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed and that information that is relevant to the commission of the offence, including the whereabouts of any person, can be obtained through the use of a tracking device, may at any time issue a warrant authorizing a peace officer or a public officer … and who is named in the warrant (a) to install, maintain and remove a tracking device in or on any thing, including thing carried, used or worn by any person; and (b) to monitor, or to have monitored, a tracking device installed in or on any thing.*

(2) *A warrant issued under subsection (1) is valid for the period, not exceeding sixty days, mentioned in it.*

(3) *A justice may issue further warrants under this section.*

(4) *For the purposes of this section, "tracking device" means any device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.*

…

Covert Surveillance: "Entitled to" reasonable expectation of privacy

37. 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*". The dictionary definition of "*entitled*" is where the person is given a rightful claim to something. It is clumsy wording and does not acknowledge the rights, including the right to privacy, that a person has under the Basic Law of the HKSAR and the ICCPR.

38. The test to be applied is whether a person had a right to privacy in particular circumstances: did he or she have a "reasonable expectation of privacy". This is the language of the courts which have looked at this right: the European Court of Human Rights in Halford v United Kingdom (1997)

24 EHRR 523, paragraph 45; the House of Lords in Campbell v MGN Ltd [2004] 2 AC 457, paragraph 21, per Lord Nicholls; and the Supreme Court of Canada in R v Wong (supra) p 465E-F, p 478A-B. In HKSAR v Chan Kau Tai (unreported, 26 January 2006, CACC 26/2004), the Hong Kong Court of Appeal applied these cases at paragraph 102 and held that: "*A right to privacy will generally exist where the person in question has a reasonable expectation of privacy, this being the test that finds favour in both the United Kingdom…and in Canada…*".

39. The infelicitous use of "entitled to" is not necessarily a mere drafting problem. The proposed regime in respect of covert surveillance envisages an executive authorization by a senior law enforcement officer, upon application by a junior investigating officer. It also envisages an emergency authorization by a head of department, upon application by a junior investigating officer. If the junior investigating officer does not believe that the targeted person is entitled to a reasonable expectation of privacy, then no authorization would be sought. This would mean that junior investigating officers could easily circumvent the provisions of the Bill as a result of their own perception about another person's reasonable expectation of privacy. The phrase "*reasonable expectation of privacy*" is something that only a court can decide after considering all the circumstances. Risks of unauthorized interferences with the right to privacy will stem from the unskilled and subjective perceptions of an investigating officer, who will not be, and cannot be expected to be, knowledgeable about human rights.

Covert Surveillance: Activities in public places

40. 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) includes "*all piers, thoroughfares, streets, roads…ways and places to which the public have access either continuously or periodically, whether the same are the property of the*

*Government or of private persons*" but exclude public toilets or bathing or changing facilities.

41. Clause 2(2) seems, therefore, 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. The reasoning of Clause 2(2) indeed suggests that anyone who wears a short skirt in the street should reasonably expect others to take photographs up her skirt, conduct which at present attracts a usual sentence of 14 days' imprisonment. See HKSAR v Yu King Man (unreported, 6 October 2004, HCMA 808/2004) (Court of First Instance).

42. The Bar considers that Clause 2(2) violates Article 39 of the Basic Law of the HKSAR and Article 17(2) of the ICCPR (right to privacy). A person has a "reasonable expectation of privacy" even in a public place. In R v Wong (supra), Chief Justice Lamer said at pp 465H-466A:

*The nature of the place in which the surveillance occurs will always be an important factor to consider in determining whether the target has a reasonable expectation of privacy in the circumstances. It is not, however, determinative. A person who is situated in what would normally be characterized as a public place (a restaurant, for example) may well have a reasonable expectation of privacy. For example, he or she would not reasonably expect that the police will surreptitiously monitor and record the private conversations taking place at his or her table.*

43. In HKSAR v Chan Kau Tai (supra), the Hong Kong Court of Appeal set out the definition of "privacy", and said at paragraph 102:

*Thus, for example, a conversation with a friend on the street can be said to involve some element of privacy as will obviously activities within one's own home*.

The Court applied the dicta of Lamer CJ in R v Wong (supra) and found that there was no reason why a person should not be entitled to privacy in his office or workplace [paragraph 103]. These places would ordinarily be considered to be "public places", yet, under the Bill, covert surveillance could be carried out in them without an authorization.

44. In HKSAR v Li Man Tak & Ors (unreported, 22 April 2005, DCCC 689/2004), Judge Sweeney of the District Court, when ruling on the admissibility of surveillance product covertly recorded in meetings held in restaurants, rejected a submission of the prosecution that the restaurants were public places and therefore not protected by Article 30 of the Basic Law of the HKSAR, holding that "*[the Basic Law] was clearly designed to protect privacy of communications rather than privacy of venue*".

45. In Von Hannover v Germany (2005) 40 EHRR 1, the European Court of Human Rights reiterated that the concept of private life under the European Convention on Human Rights "*extends to aspects relating to personal identity, such as a person's name … or a person's picture*" and private life –

"*includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings … There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'…*" (paragraph 50).

The European Court proceeded to hold that the publication by various German magazines of photographs of Princess Caroline of Monaco in her daily life (such as dining in a restaurant, shopping at the market, on a skiing holiday, leaving her house, and tripping over in the premises of a club) "*falls within the scope of her private life*" (paragraph 53).

46. Legislation cannot limit the right to privacy guaranteed by the Basic Law of the HKSAR and the ICCPR. It is the constitution that forms the law, the law does not form the constitution. As Bokhary PJ indicated in Prem Singh v Director of Immigration [2003] 1 HKLRD 550 (Court of Final Appeal) at paragraph 8 that: "*Basic Law rights and freedoms are neither dependent upon nor defeasible by ordinary law*." Clause 2(2) is based upon an erroneous understanding of the right to privacy. It is also an overt attempt of the Administration to overturn unfavourable and inconvenient jurisprudence. It is further 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

47. 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.

48. A reading of the Theft Ordinance (Cap 210) is instructive. The offence of robbery carries a maximum penalty of imprisonment for life. The offences of theft, obtaining property by deception, and false accounting: 10 years' imprisonment. Taking conveyance without authority: 7 years' imprisonment. Abstracting of electricity: 5 years' imprisonment. Making off without payment and going equipped for stealing: 3 years' imprisonment. Dishonest use of the public telephone system: 2 years' imprisonment.

49. Further, the following offences carries a maximum sentence of 3 years' imprisonment upon conviction on indictment or summarily:

- Public Order Ordinance (Cap 245) section 17A(3) (offences associated with organization of unauthorized assembly), section 18 (unlawful assembly);
- Registration of Local Newspapers Ordinance (Cap 268) section 20(1) (any offence under the Ordinance);
- Road Traffic Ordinance (Cap 374) section 37 (dangerous driving);
- Regional Flag and Regional Emblem Ordinance (117 of 1997) section 7 (desecration of the regional flag or regional emblem).

50. The Bill's scope of "serious crimes" is far too broad. The Bill should cover only the most serious offences so that the interference with privacy is proportional.

51. In Australia, sections 5 and 5D of the Telecommunications (Interception) Act 1979 together provide a comprehensive list of criminal offences, defined by specified descriptive categories, to which the Act applies. They include –

- Offences of murder, kidnapping, acts of terrorism;
- Offences punishable by imprisonment for life or for a period of at least 7 years and the particular conduct constituting the offence involved, involves or would involve, as the case requires, loss of a person's life or serious risk of loss of a person's life; or serious personal injury or serious risk of serious personal injury; or serious damage to property in circumstances endangering the safety of a person; or serious arson; or trafficking in prescribed substances; or serious fraud; or serious loss to the revenue; or bribery or corruption of, or by a public officer; or the production, publication, possession, supply or sale of, or other dealing in, child pornography;
- Offences punishable by imprisonment for life or for a period of at least 7 years and the offence involves 2 or more offenders and substantial planning and organization; and involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and is

committed or its of a kind that is ordinarily committed, in conjunction with other offences of a like kind; and consists of, or involves theft, handling stolen goods, tax evasion, extortion, bribery or corruption of, or by a public officer, dealings in firearms or armaments, etc;

- Offences involving money laundering; and
- Offences characterized as cybercrimes by reference to specific legislative provisions.

52. In Canada, section 183 of the Criminal Code permits the interception of private communications for a list of specified offences. In New Zealand, section 312A(1) of the Crimes Act 1961 sets out "serious violent offences" and a "specified offence" – offences punishable by 10 years' imprisonment or more, and listed offences. In the United States, section 2516(1) of Title 18, United States Code, sets out a long list of offences.

53. In Hong Kong, the powers of investigation in sections 3 to 5 of the Organized and Serious Crimes Ordinance (Cap 455) ("OSCO") are only for listed offences in Schedules 1 and 2 of that Ordinance. That list was compiled after taking into account representations of the police force, the ICAC and the Customs & Excise Service, and was to ensure that the powers were limited to those offences which represented a real problem to Hong Kong and for which the powers were needed.

54. 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.

<u>Conditions for Prescribed Authorization: Public Security</u>

55. The Bill prescribes as a legitimate purpose for obtaining a prescribed authorization the purpose of protection of "public security" (gonggonganquan): Clause 3(1)(a)(ii).

56. 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". The ICAC, the Customs and Excise Service and the Immigration Department each have subject-defined closed statutory remits. The police force has a list of specific and general duties under section 10 of the Police Force Ordinance (Cap 232). An express duty to protect "public security" is not amongst them. The Administration therefore should explain how it intends officers of "departments" as defined in Clause 2(1) deciding on whether a particular problem not involving the prevention or detection of a serious crime is a matter of "public security" within the officer's statutory remit of functions. The response of the Security Bureau in Legislative Council Paper on Response to issues raised by Members at the meeting of 7 February 2006 of the Security Bureau (February 2006) paragraphs 2 to 3 is very vague.

57. The expression "public security" has up to now been used in only 1 context in Hong Kong legislation, namely as a ground for the Administration to take over the operation of franchised tunnels or harbour crossings "in the interest of public security"; see Eastern Harbour Crossing Ordinance (Cap 215) section 49; Tate's Cairn Tunnel Ordinance (Cap 313) section 30; Western Harbour Crossing Ordinance (Cap 426) section 27; and Tai Lam Tunnel and Yuen Long Approach Road Ordinance (Cap 474) section 22. However, the expression has been translated as "gongzhonganquan" in Chinese in those provisions.

58. The expression of "gonggonganquan" is provided as the Chinese equivalent for the expression of "public safety" in Article 17 of the Hong Kong Bill of Rights and section 2(2) of the Public Order Ordinance (Cap 245). It should be noted that the expression of "public safety" is derived from Article 21 of the ICCPR, which provides that the right of peaceful assembly may only be restricted by measures that are "*necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others*". In Nowak, *UN*

*Covenant on Civil and Political Rights: CCPR Commentary* (Kehl and Arlington: N P Engel, 1993), "national security" as a ground for restriction is confined to "*serious cases of political or military threat to the entire nation*", whereas "public safety" is referred to in the context of "*a specific threat to the safety of persons (i.e. their lives, their physical integrity or health) or things*" (p 380).

59. The Bill incorporates the protection of "public security" as a legitimate purpose for obtaining a prescribed authorization because of the language of Article 30 of the Basic Law of the HKSAR, which provides as an exception to the prohibition of infringement of freedom and privacy of communication the inspection of communication by the relevant authorities in accordance with legal procedures to meet the needs of "public security" (gonggonganquan).

60. The wording of Article 30 of the Basic Law of the HKSAR 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).

61. The concept of "public security" in Article 30 of the Basic Law of the HKSAR is a nebulous one. There are at least 2 questions in this connection. The first is whether the concept of "public security" (gonggonganquan) is identical to or wider than that of "state security" (guojiaanquan). The second is whether the concept of "public security" should, by reason of the drafting history of the Basic Law, be understood as "state security" (guojiaanquan) is understood in Mainland China or as "national security" is understood in international human rights jurisprudence.

62. A study of Mainland law indicates that "public security" (gonggonganquan) is a concept distinct from that of "state security" (guojiaanquan). See, for example, Criminal Law of the People's Republic of China, Part II, Chapter 1 (Crimes Endangering State Security (Guojiaanquan)) and Chapter 22 (Crimes Endangering Public Security (Gonggonganquan)). See also other

national legislations such as the Martial Law, Article 2 and the Law on Meetings, Processions and Demonstrations of the People's Republic of China, Article 12.

63. It is difficult to imagine what is intended by the protection of "public security" (gonggonganquan) which would not be covered by the prevention or detection of "serious crime".

64. The judgment of the Hong Kong Court of Final Appeal in Leung Kwok Hung & Ors v HKSAR [2005] 3 HKLRD 164 is illustrative of the flaw of grafting onto legislative text delimiting conditions for exercise of discretionary powers an insufficiently certain concept taken from a human rights or constitutional instrument. The fact that Article 30 of the Basic Law of the HKSAR mentions "public security" (gonggonganquan) is not necessarily a good and sufficient reason for incorporation.

65. 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

66. 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

67. Clause 3(1)(b) prescribes a test of proportionality that requires consideration of the matters set out in sub-paragraphs (i) and (ii). Sub-paragraph (i) prescribes the conduct of a "balancing" of "relevant factors" (which are concerned with the immediacy and gravity of the crime or threat and the likely value and relevance of the information likely to be obtained by the proposed activity) "in operational terms".

68. The test of proportionality thus prescribed 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 among panel judges; as between panel judges on the one hand, and heads of departments and authorized officers on the other; and among authorized officers of different departments. Such inconsistencies in approach may be subtle and difficult to discover. Panel judges are apparently not permitted to have access to each other's determinations (which are presumably to be secured as part of the relevant sealed packet). The Commissioner does not appear to be in a position to have a complete overview of all the activities provided for under the Bill, since, for example, his functions under Clause 39 are directed towards departments and he does not have automatic and direct access to determinations of panel judges.

69. The Administration should explain the need to insert into the test of proportionality test the qualifying term of "in operational terms". It is not

inconceivable that especially in the context of executive authorization, this term may be interpreted to produce a structural bias in favour of the operational needs and convenience of the law enforcement agencies.

Legal Professional Privilege

70. One of the greatest threats to the Rule of Law is the interception of communications and covert surveillance of lawyers, for example recording their conversations with clients. "*A man must be able to consult his lawyers in confidence, since otherwise he might hold back half the truth. The client must be sure that what he tells his lawyer in confidence will never be revealed without his consent*": R v Derby Magistrates Court ex p B [1996] AC 487 (House of Lords) at 507 (per Lord Taylor CJ). Lawyers must be assured that their communications will be privileged and not recorded and examined.

71. Legal professional privilege is a constitutional right. Article 35 of the Basic Law of the HKSAR provides that "*Hong Kong residents shall have the right to confidential legal advice*". It is recognized as "*one of the pillars upon which the administration of justice in Hong Kong rests. … Any encroachment on [legal professional privilege] therefore affects not just the legal system but has an impact too on the broader public interest*". See Pang Yiu Hung Robert v Commissioner of Police [2002] 4 HKC 579 (Court of First Instance). It is a right which the HKSAR courts will always be vigilant to accord proper protection: A Solicitor v Law Society of Hong Kong (unreported, 22 March 2006, FACV 23/2005) (Court of Final Appeal) at paragraph 15 (per Bokhary PJ).

72. The Bill envisages that interception of communications and covert surveillance may be carried out against lawyers. Clause 2(3) reads:

> *(2) For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of "Type 2 surveillance" in subsection (1) is regarded as Type 1 surveillance if it is likely*

*that any information which may be subject to legal professional privilege will be obtained by carrying it out.*

This provision leaves it to the public officer to determine whether it is "*likely*" that legal professional privileged communications will be obtained. If he is wrong in his assessment and only obtains an "executive authorization", and legal professional privileged communications are in fact obtained, then such communications will be known to the investigating officers. That is not an adequate protection. All safeguards must be taken so as to ensure that no legal professional privileged communications are recorded.

73. The Bill does not afford sufficient protection that legal professional privileged communications will not be interfered with, recorded and examined. 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 the authorization that may record such communications.

74. In Canada, under section 186(2) of the Criminal Code no authorization may be given to intercept the private communication at the office or residence of a solicitor (i.e. lawyer), or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients,

*…unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other solicitor or a member of the solicitor's household has been or is about to become a party to an offence.*

That provision may not be sufficient: it does not cover a lawyer meeting a client at a restaurant to discuss legal matters, which frequently happens. The lawyer could give legal advice using a mobile phone in his or her

vehicle. It focuses on a place where the communications will take place, i.e. the solicitor's office or barrister's chambers.

75. In New Zealand, section 312C(1)(d) of the Crimes Act 1961 provides that upon an application for an interception warrant, the judge must have reasonable grounds for believing that:

> *(d) the private communications to be intercepted are not likely to be privileged…*

This puts the onus on the applicant to show that legal professional privileged communications will be protected.

76. In Hong Kong, the United Nations (Anti-Terrorism Measures) Ordinance (Cap 575) provides in section 2(5) that:

> *Nothing in this Ordinance shall –*
>
> *(a) require the disclosure of any items subject to legal privilege;*
> *(b) authorize the search or seizure of any items subject to legal privilege; or*
> …

This provision applies to restrict the extensive and court-sanctioned powers of investigation under that Ordinance (which are inserted in 2004 but are not yet in operation).

77. The Administration should justify with cogent reasons why it does not exclude legal professional privileged communications from being the object of prescribed authorizations to be made under the Bill.

78. Under the Bill, a public officer making an application for a prescribed authorization is only required to state in an affidavit "*the likelihood that any information which may be subject to legal professional privilege will*

*be obtained by carrying out the interception*"; see Schedule 3, Part 1, paragraph (b)(viii); Part 2, paragraph (b)(ix); and Part 3, paragraph (b)(ix). The extent of disclosure indicated in these provisions does not appear to require detailed disclosure of information that might show by reference to circumstances, location and parties that a conversation or communication in another form is likely to be a communication that is subject of legal professional privilege. These provisions do not provide any adequate safeguard.

79. 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.

80. 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. See the Crimes Act 1961 of New Zealand, section 312D(2).

81. The Administration should amend the Bill to preserve the character of communications under legal professional privilege, notwithstanding that such communications have been 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. See the Canadian Criminal Code, section 189(6) and the Crimes Act 1961 of New Zealand, section 312O, which states as follows –

*Where evidence obtained by the interception of a private communication would, but for the interception, have been privileged by virtue of –*

…

*(b) Any rule of law that confers privilege on communications of a professional character between a barrister or solicitor and a client, -*

*such evidence shall remain privileged and shall not be given in any Court, except with the consent of the person entitled to waive that privilege.*

82. 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.

83. 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

84. Non-compliance with any of the substantive provisions of the Bill should be a criminal offence. The fact that the criminal sanctions are not provided for generally is not a good reason for not doing so.

85. In other jurisdictions, the interception of private communications; or the carrying out of covert surveillance which involves the recording of

conversations, without an authorization, is an offence; see in Canada, section 184 of the Criminal Code; in the United Kingdom, section 1 of the Regulation of Investigatory Powers Act 2000.

86. It is considered that the Administration would not have argued for immunity from criminal liability were the legislation one of general application. The suggested criminal wrongdoing of "misconduct in public office" is not necessarily entirely appropriate. Transgressions of some of the provisions of the Bill may not be sufficiently serious to allow for prosecution for this serious common law offence but may require criminal sanctions all the same, for example, negligent disclosure of the fact of an authorized intercept or negligent keeping of protected products (Clause 56) or records (Clause 57).

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

87. Clause 6 proposes that "judicial authorization" of interception of communications and Type 1 surveillance will be undertaken by panel judges (who are judges of the Court of First Instance) appointed by the Chief Executive upon recommendation by the Chief Justice.

88. The panel judges are to consider written applications made by officers of the relevant departments for authorization and deliver written determinations issuing, with or without variations, the authorization sought in the application, or refusing to issue the authorization sought: Clauses 7, 8. The panel judges also are to consider written applications made by such officers for confirmation of an emergency authorization: Clause 23. Applications for authorization may be made orally if it is considered that in all the circumstances of the case it is not reasonably practicable to make a written application: Clause 25. A prescribed authorization that was issued orally by a panel judge needs to be confirmed by way of a written application to the panel judge: Clause 26. The panel judges further are to consider written applications for a device retrieval warrant: Clause 32.

89. The panel judges are to consider the applications for authorization in private, and may do so in a place other than within the court precincts: Schedule 2, paragraph 1 of the Bill.

90. The panel judges are empowered to administer oaths and take affidavits for the purpose of performing any of their functions under the Bill: Schedule 2, paragraph 2 of the Bill.

91. Schedule 2, paragraph 4 of the Bill states:

*In performing any of his functions under this Ordinance, a panel judge shall act judicially and have the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court.*

Schedule 2 may be amended by the Chief Executive in Council by notice in the Gazette: Clause 63.

92. The above provisions suggest that the Administration proposes to confer upon the panel judges in their personal capacities an administrative power, to be exercised judicially. Accordingly, it can be said that the scheme of authorization proposed for interception of communications and Type 1 surveillance is one of executive authorization by judges.

93. 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 the Chief Justice to appoint two other judges of the

Court of First Instance to hear the application. Only judges of the Court of First Instance nominated by the Chief Justice may hear applications for judicial review. 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.

94. 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.

95. The Administration must assure the public that the new legislation will not impair the operational efficiency of the Judiciary and the law enforcement agencies. It is unacceptable that because judges may accept responsibilities offered to them under the Bill judicial resources are thereby depleted. The Administration must ensure that does not happen.

96. There is no reason why Schedule 2, paragraph 4 of the Bill, which is apparently concerned with the fundamental issue of the legal capacity of panel judges in the exercise of their statutory functions under the Bill, is stated in Clause 63 to be capable of amendment by the Chief Executive in Council, without vetting by the Legislative Council. Schedule 2, paragraph 4 should be re-positioned to the body of the Bill.

97. The wording of Schedule 2, paragraph 4 of the Bill is problematic from the perspective of separation of powers. Articles 2, 19 and 80 of the Basic Law of the HKSAR vests the independent judicial power of the HKSAR upon the Judiciary of the HKSAR. There is no necessary inconsistency with the separation of powers if non-judicial power is vested in individual judges detached from the court they constitute. The power to confer non-judicial functions on judges as designated persons is subject to the conditions that the conferral must be consented to by the judge and the function must not be incompatible either with the judge's performance of

judicial functions or with the proper discharge by the Judiciary of its responsibilities as an institution exercising independent judicial power; see Grollo v Palmer (1995) 184 CLR 348 (High Court of Australia). See also Mistretta v United States 488 US 361 (1989) (United States Supreme Court).

98. 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. In this connection, section 12 of the Surveillance Devices Act 2004 from Australia is instructive:

> *(1) In this section, unless the contrary intention appears:*
> ***eligible Judge*** *means a person in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force.*
> ***Judge*** *means a person who is a Judge of a court created by the Parliament.*
> *(2) A Judge may, by writing, consent to be declared an eligible Judge by the Minister under subsection (3).*
> *(3) The Minister may, by writing, declare Judges in relation to whom consents are in force under subsection (2) to be eligible Judges for the purposes of this Act.*
> *(4) Any function or power conferred on the Judge under this Act is so conferred only in a personal capacity and not as a court or a member of a court.*
> *(5) An eligible Judge has, in relation to the performance or exercise of a function or power conferred on an eligible Judge by this Act, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.*
> …

As presently drafted, Clause 6 and Schedule 2, paragraph 4 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.

99. 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 is not a form of enlistment. Rather it implies a continuing 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. In Grollo v Palmer (supra), the judgment of Brennan CJ, Deane, Dawson and Toohey JJ provides at p 365 an indication of the ways in which the performance of non-judicial functions by judges may become incompatible:

*Incompatibility might consist in so permanent and complete a commitment to the performance of non-judicial functions by a judge that the further performance of substantial judicial functions by that judge is not practicable. It might consist in the performance of non-judicial functions of such a nature that the capacity of the judge to perform his or her judicial functions with integrity is compromised or impaired. Or it might consist in the performance of non-judicial functions of such a nature that public confidence in the integrity of the judiciary as an institution or in the capacity of the individual judge to perform his or her judicial functions with integrity is diminished.*

In Mistretta v United States (supra), Blackmun J, writing for the 8-1 majority, warned at p 407 that:

*While the problem of individual bias is usually cured through recusal, no such mechanism can overcome the appearance of institutional partiality that may arise from judiciary involvement in the making of policy. The integrity of the Judicial Branch ultimately depends on its reputation for impartiality and nonpartisanship. That reputation may not be borrowed by*

*the political Branches to cloak their work in the neutral colours of judicial action.*

This continuing obligation, the Administration should remember, is a constitutional one, for which it can be held accountable before the courts of the HKSAR, whether in a dedicated legal challenge or incidentally in the course of a criminal prosecution. The Administration should not, in discharging this obligation, forget the words of Mortimer V-P in Wong Yeung Ng v Secretary for Justice [1999] 2 HKC 24 at 44G-H:

*Confidence in our legal system, the maintenance of the rule of law and the authority of the court are matters of special importance in our society. There are frequent, if misconceived, expressions of anxiety in this respect. There is reason to believe that the ordinary citizen in Hong Kong regards the court as his ultimate and sure refuge from injustice and oppression.*

100. 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 in which the Administration claims public interest immunity from disclosure of particular documents, and have to rule on the validity of the claim by considering privately such documents, except where the claim is one based on the ground of an actual or potential risk to national security, the court should not inspect the documents to which that claim relates. See *Halsbury's Laws of Hong Kong*, Vol 5(3) (2004 Reissue), [90.2384]. The present arrangement of "appointment checking" must have been put in place against this legal background. The Administration has not put forward a case to justify the imposition of the highest level of integrity checking upon panel judges candidates, a level of integrity checking even higher than that applicable to the Chief Justice and Permanent Judges of the Court of Final Appeal.

Applying for a Judicial Authorization

101. Clause 8 provides for the making of applications for judicial authorizations for interceptions of communications and for Type 1 surveillance. The application is made by an officer of the relevant department following approval by a directorate officer of that department.

102. In Hong Kong, an application for orders for persons to provide information to law enforcement agencies under section 3 of OSCO is made by the Secretary for Justice.

103. In Canada, applications for authorization for the interception of private communications must be made by authorized counsel of the Attorney General's Chambers: Criminal Code section 185. In the United States, such applications are authorized by a high ranking officer in the Department of Justice and made by prosecuting attorneys: United States Code, Title 18, section 2516(1), (2). On the other hand, in New Zealand, applications for a warrant to intercept private communications are made by the police: Crimes Act 1961 section 312B.

104. 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 who may be far more knowledgeable about human rights, and act a responsible and independent vetting authority. Approval by a directorate officer of the relevant department does not appear to be an adequate safeguard.

105. Clause 8(2) provides that an application for a judicial authorization is to be supported by an affidavit of the applicant that complies with requirements set out in Schedule 3, Part 1 or 2 (where appropriate) of the Bill.

106. The provisions in Schedule 3 of the Bill do 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.

107. An affidavit complying with Schedule 3 of the Bill requires a public officer making an application for a judicial authorization to state, inter alia:

*the reason why the purpose sought to be furthered by carrying out [the interception/ Type 1 surveillance] cannot reasonably be furthered by other less intrusive means;..*

Higher thresholds are provided in overseas jurisdictions. In Canada, section 185(1)(h) of the Criminal Code requires that the applicant must state in his affidavit in support of a wiretap authorization:

*(h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.*

Before granting the authorization the judge must be satisfied of the above: section 186(1)(b).

In New Zealand, section 312B(1)(e) of the Crimes Act 1961 requires the applicant to state that he has reasonable grounds to believe:

*(e) whichever of the following is applicable:*

*(i) the other investigative procedures and techniques that have been tried but have failed to facilitate the successful conclusion of the police investigation of the case, and the reasons why they have failed in that respect; or*

*(ii) the reasons why it appears that other investigative procedures and techniques are unlikely to facilitate the successful conclusion of the police investigation of the case,*

*or are likely to be too dangerous to adopt in the circumstances; or*

*(iii) the reasons why it is considered that that the case is so urgent that it would be impractical to carry out the police investigation using only investigative procedures and techniques other than the interception of private communications.*

Before granting the interception warrant the judge must be satisfied that it would be in the interests of justice to do so, and that he has reasonable grounds to believe or the above matters: Crimes Act 1961, section 312C.

In the United States, section 2518(1)(c) of Title 18, United States Code requires the applicant to state in his affidavit:

*(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; …*

Before granting the interception order the judge must be satisfied of the above: United States Code, Title 18, section 2516(3)(c).

108. It can be seen that the 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.

109. Turning back to Hong Kong, under section 3(3)(d)(ii) of OSCO, before the Court makes an order for a person to provide information it must be satisfied that it has reasonable grounds for believing that it is in the public interest for an order to be made, having regard "*to whether or not the organized crime could be effectively investigated if an order*" was not made. In respect of an order for the search and seizure of "journalistic material" under Part XII of the Interpretation and General Clauses

Ordinance, before a judge makes an order under section 84(3) he must be satisfied that there are "*reasonable grounds for believing*", amongst other things,:

> *(d) other methods of obtaining the material –*
>
> *(i) have been tried and failed; or*
>
> *(ii) have not been tried because they were unlikely to succeed or would be likely to seriously prejudice the investigation;…*

It can be seen that the requirements under OSCO section 3 and the 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.

110. It must be emphasized that panel judges rely on the information provided in the affidavit in support 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. Those facts might be wrong. They might be deliberately misstated. They might be innocently misstated. 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.

111. In addition, in Schedule 3, Part 1 of the Bill, an application for a judicial authorization needs to state under (b) merely: "*if known, the identity of any person who is to be the subject of the interception*". This is not sufficient. Fuller particulars about the person, for example, his address and occupation should be included. The latter will assist the judge in determining whether legal professional privilege may be of a concern.

112. Fuller particulars are required in overseas jurisdictions. In Canada, under section 185(1)(e) of the Criminal Code, the applicant must state:

> *(3) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,*

In New Zealand, under section 312C(2)(c)(i) of the Crimes Act 1961, the applicant must state:

> *(c) either, -*
>
> *(i) if they are known, the name and address of the subject the interception of whose private communications there are reasonable grounds for believing will assist the police investigation of the case…*

113. The Administration should explain why it is proposed that legal enforcement agencies in Hong Kong are not to be required to provide fuller particulars.

<u>Determining an Application for Judicial Authorization</u>

114. Clause 9 contains no specific requirement for the panel judge to direct himself as to the inclusion of any conditions to minimize the interference with the right to privacy. It just states that the panel judge, may issue the judicial authorization sought, "*with or without variations*". Clause 31 merely states that an authorization may be issued subject to any conditions specified in it that apply to the authorization itself or to any further authorization or requirement under it.

115. 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, bearing in mind the extensive terms that the Bill proposes to permit an authorization to contain or further authorize; see Clauses 29, 30.

116. In Canada, under section 186(4)(d) of the Criminal Code, the authorization shall "*contain such terms and conditions as the judge considers advisable in the public interest; …*". In New Zealand, under section 312D of the Crimes Act 1961, there is a similar provision. It goes further, and in section 312D(2) states:

> *(2) Without limiting the generality of subsection (1), where it is proposed to place an interception device in the residential or business premises of a person who is a barrister or solicitor, or a clergyman, or a medical practitioner, the Judge shall prescribe such conditions (if any) as the Judge considers desirable to avoid so far as practicable the interception of communications of a professional character to which the barrister or solicitor or clergyman or medical practitioner is a party.*

Duration and Renewal of Judicial Authorization

117. A judicial authorization issued under Clause 10(b) is in effect for up to 3 months. Renewals are for the same period: Clause 13(b).

118. Shorter periods of authorization are provided in overseas jurisdictions. In Canada, under section 186(4)(e) of the Criminal Code, authorizations for the interception of private communications are for up to 60 days (except for terrorism offence). In New Zealand, under section 312D of the Crimes Act 1961, interception warrants are valid for up to 30 days. In the United States, under section 2518(5) of Title 18, United States Code, a 30 day period is applicable for interception orders.

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

120. 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. Schedule 3, Part 4, paragraph (a)(iv) of the Bill only requires an applicant for renewal of an authorization to state "*the reason why it is necessary to apply for the renewal*". 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.

121. The information proposed to be set out in an affidavit in support of an application for renewal under Schedule 3, Part 4, paragraph (a) of the Bill, such as *"(iii) the value of the information so far obtained pursuant to the judicial authorization …*", does not appear to provide the full extent of information relevant to the assessment by a panel judge. In Canada, where an application is made for a renewal of an authorization to intercept communications, section 186(6) of the Criminal Code requires the affidavit in support to depose to the following matters:

*(a)* *the reason and period for which the renewal is required;*

*(b)* *full particulars, together with times and dates, when interceptions, if any, were made or attempted under the authorization, and any information that has been obtained by any interception; and*

*(c)* *the number of instances, if any, on which, to the knowledge and belief of the deponent, an application has been made under this subsection in relation to the same authorization and on which the application was withdrawn or no renewal was given, the date on*

*which each application was made and the name of the judge to whom each application was made,*

*and supported by such other information as the judge may require.*

In New Zealand, section 312F of the Crimes Act 1961 requires the giving of similar particulars in an application for the renewal of an interception warrant.

Executive Authorizations

122. The Bar's views on the contents of the affidavit to be prepared for an application for a judicial authorization above apply equally to the contents of the statement to be prepared for an application for an executive authorization.

123. The Bar's views on the issues of specifying conditions in a judicial authorization and the duration of an authorization or its renewal apply equally to an executive authorization.

124. Clause 17 provides that renewals of an executive authorization issued under Clause 15 may be sought from an authorizing officer of the same department.

125. 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

126. Clauses 29(6) and (7) provide for activities that a prescribed authorization for interception or covert surveillance "also authorize". Such activities include: "*the entry, by force if necessary, onto any premises in order to carry out any conduct authorized or required to be carried out under the*

*prescribed authorization*". Contrast with the provisions in Clauses 29(1) to (5), which provides that a prescribed authorization "may contain terms that …".

127. The Administration should explain why it does not draft Clauses 29(6) and (7) in the way Clauses 29(1) to (5) are drafted so that the activities covered in Clauses 29(6) and (7) are only authorized upon the conscious decision of the relevant authority.

128. 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" is very broad. They might arguably be applied to cover arbitrary activities. No "further authorization" in similar terms is provided for in Canadian and New Zealand legislation in this field. Given that authorizations issued pursuant to the Bill encroaches upon what would otherwise be a person's freedom of communication and privacy protected under the Basic Law of the HKSAR and the ICCPR, and that such encroachment should be minimized to preserve the fundamental rights concerned, the present formulation of the generality portion of this clause is most inappropriate.

129. Clause 30 also lists a number of activities that is sought to be "further authorized", including –

- such interference with private property as "*the temporary removal of any conveyance or object from any premises for the installation, maintenance or retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises*" (paragraph (c)), "*the breaking open of anything for the installation, maintenance or retrieval of the devices or enhancement equipment*" (paragraph (d)), and

• "*the connection of the devices or enhancement equipment to any source of electricity and the use of electricity from that source to operate the devices or enhancement equipment*" (paragraph (e)).

130. 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.

Emergency Applications

131. Clause 20 makes provision for emergency authorizations for interception of communication and Type 1 surveillance by the head of a department. The Administration should justify its refusal to entrust emergency applications to panel judges, bearing in mind that applications may be made orally.

132. In Canada, emergency applications for authorization to intercept private communications are made to a judge designated from time to time by the Chief Justice or senior judge of the relevant province or territory, as the case may be, pursuant to the Criminal Code, section 188. In New Zealand, emergency permits for the interception of private communications are given by a judge under the Crimes Act 1961, section 312G.

133. 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 to be made by the head of a department. Such authorizations will be easy to justify when compared with the other criteria, which relate to death or serious bodily harm to persons, substantial damage to property or serious threat to public security. The mere possibility of the loss of vital evidence does not appear to be a proportionate reason for emergency authorizations of interception of communications or Type 1 surveillance.

134. In Australia, section 30 of the Surveillance Devices Act 2004 limits the circumstances in which an emergency authorization for the use of a surveillance device may be made to prevent a loss of relevant evidence to investigations into a number of specified offences, such as treason, espionage, terrorism, slavery, and trafficking of narcotic drugs and psychotropic substances.

135. In Canada, under section 184.4 of the Criminal Code, a police officer may intercept private communications in urgent situations where the obtaining of a judicial authorization could not be obtained and in circumstances of preventing serious harm to any person or property.

Notification

136. There is no provision in the Bill that requires law enforcement agencies to notify a person who has been the object of an interception of his communications or covert surveillance after the investigation. Unless the person is informed about this, he is not in a position to complain to the Commissioner; or, if he is an accused, to properly prepare his defence.

137. 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 decided to pursue whatever remedy is available.

138. In Canada, section 196 of the Criminal Code requires the Attorney General of Canada or of the province, within 90 days after the period for which the authorization was given or renewed, or within such other period fixed by a judge, to notify in writing the person who was the object of the interception pursuant to an authorization. Under section 196(2) and (3), an application can be made to a judge to extend the period up to three years, for example, where an investigation is continuing and the judge is of the opinion that the interests of justice warrant granting the application.

Civil Immunity

139. In general, civil liability for unlawful activities carried out in contravention of the Bill or carried out in association with a prescribed authorization or device retrieval warrant should act as a deterrent against abuse.

140. The immunity provisions in Clause 61 appear to be too wide. Only Clause 61(1)(a) alone is acceptable. Interception of communications and covert surveillance are severe intrusions into privacy. If mistake is no answer to an action in trespass under an invalid warrant (which is a principle recognized in Clause 61(2)), it should likewise applies to an interception of communication that is made on a mistaken basis coming within Clause 61(1)(a) or (b).

The Commissioner on Interception of Communications and Surveillance

141. 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.

142. Clause 53, in prescribing that the Commissioner "*is for all purposes not regarded as a court or a member of a court*" in performing any of his functions under the Bill, 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. Accordingly, the Bar's comments above on the constitutional position of panel judges equally apply to a Commissioner whose eligibility derives from his current service as a judge. Clause 38 should as a result be suitably amended.

143. 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 in the context of

interception of communications and covert surveillance. Firstly, how does a person begin to believe that his communications have been intercepted or his conversations and movements kept under covert surveillance if he is not informed of any such activity having been practised upon him. Secondly, the person must "*believe*" that his communications have been intercepted or conversations and movements kept under covert surveillance. This is a high mental threshold for the person to have. A threshold of "*suspect*" would be more appropriate. See Gifford v Kelson [1943] 3 DLR 441 (King's Bench, Manitoba); Johnson v Whitehouse [1984] RTR 38 (Queen's Bench Division, England); and *Halsbury's Laws of Hong Kong*, Vol 9 (2002 Reissue) [130.604].

144. 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".

145. Under Clause 43(2)(b), the Commissioner may order the payment of compensation to the applicant. This cannot prevent a person bringing a civil suit for breach of his right to privacy: Watkins v. Secretary of State for the Home Department and Ors [2005] QB 883 (English Court of Appeal: misfeasance in public office interfering with person's constitutional right). In the United States, under section 2520 of Title 18, United States Code, a person whose communications has been intercepted, etc, may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

146. The Commissioner should not be constrained in his examination functions by the straitjacket of "principles applicable to judicial review": Clause 45(1)(a). Very experienced judges do not, and do not want to, second guess decision-makers but they may wish to look very closely at decision-making and express a view on the merits of a decision because the circumstances call for it. In any event, in cases involving human rights, which cases on interception of communications or covert surveillance are,

judges can subject decisions to "intense scrutiny". See, for example, R v Ministry of Defence ex p Smith [1996] QB 517 (English Court of Appeal). The Administration should be willing to make the activities of law enforcement agencies open to proper audit and not keep the Commissioner at arm's length.

147. The Commissioner is to make a report to the Chief Executive pursuant to Clause 47. The contents of the report are set out in Clause 47(2). A copy of the report is to be provided to the Legislative Council: Clause 47(4). The requirements as to the content of the report are too limited. For example, the report does not have to state the number of persons who were the objects of the authorizations, or the number of criminal investigations commenced, or the number of prosecutions instituted as a result of the authorizations. This is the type of comprehensive information that the Chief Executive and the Legislative Council require in order to see if the law is being abused or is effective.

148. The contents of similar reports in overseas jurisdictions give far more information about the use of interception of communications and covert surveillance, and should be looked at as models: in Canada, Criminal Code section 195; in New Zealand, Crimes Act 1961, section 312Q; and in the United States, United States Code, Title 18, section 2519.

Effective Remedies

149. The right of HKSAR residents to effective remedies for violations of their fundamental rights is enshrined under Article 35 of the Basic Law of the HKSAR (the right to judicial remedies) and Article 3 of the ICCPR (the right to effective remedies).

150. 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 of communications or surveillance. The Court of First Instance is disinclined to entertain an application for judicial review in the absence of facts that merits investigation. In any event, the Court of First Instance does not entertain an application for judicial review where there is an alternative avenue for remedy, which in the present context, is an application to the Commissioner for examination. The resident, however, will find himself in a double bind since he must state in the application that he "believes" that interception of communications or surveillance was carried out against him and the Commissioner is empowered to refuse to examine his case if he considers that having regard to all the circumstances of the case, the application is frivolous or vexatious or is not made in good faith (Clause 44(1)(d)).

Code of Practice

151. The Code of Practice should be laid before the Legislative Council like the comparable codes of practice made under section 71 of the Regulation of Investigatory Powers Act 2000. The Code(s) of Practice should address similar issues to the issues addressed in the codes of practice in the United Kingdom so that:

(a) The public have an idea of the parameters of their right to privacy and the circumstances when there may be interference with those rights under the law.
(b) The public know the yardstick which the Commissioner measures the performance of law enforcement agencies under the legislation.

152. The Administration may wish to confirm that there will be only one Code of Practice. It is noted that manuals dealing with techniques of interception of communications or covert surveillance are to be dealt with differently.

Disclosure

153. Consultation of the membership of the Bar indicates that there is a strong body of opinion among the experienced members practising in criminal law that notwithstanding the intention of the Administration indicated in Clause 58(1) not to have any telecommunications interception product admissible in any proceedings before any court, the defence in criminal proceedings should, contrary to what is stated in Clause 58(2), have access to it, and, contrary to what is stated in Clause 58(1), 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 of the HKSAR and the ICCPR, and a common law right that the courts will safeguard jealously. There is an arguable case to say that the need to protect the right to a fair trial outweighs the need to protect the right to privacy of others caught up in the interception of communications or covert surveillance.

154. The Administration, having made the policy decision in Clause 58(1) that intercepts and intercepted material will play no part in proceedings in a court, proposes to provide in Clause 58(4) exceptions to this rule. Clause 58(4) as presently formulated, seriously limits the prosecution's duty of disclosure under common law. In Clause 58(4)(a) it permits disclosure to the prosecutor to allow him to determine "*what is required of him by his duty to secure the fairness of the trial of that offence*", and under (b) to a judge who has ordered the disclosure to himself. In respect of (a), this leaves it to the prosecutor to decide what should be disclosed. If he does not think a matter needs to be disclosed to secure a fair trial, nobody will know about it, not even the trial judge. It is not for the prosecutor to have the final say as to what is required for a fair trial; that determination is for a judge.

155. In respect of (b), the judge will only order disclosure to himself if he is satisfied that it is essential in the interests of justice. That is arguably a test with a high threshold: a more appropriate test may be "in the interest of a fair trial".

156. Given that section 18 of the Regulation of Investigatory Powers Act 2000 of the United Kingdom makes provision for about 15 exceptions, the Administration should confirm that there are good legal policy reasons for not countenancing any more exceptions.

157. Clause 58(6) provides that where the judge orders disclosure under Clause 58(4)(b), he may direct the prosecutor to "*make for the purposes of the proceedings any such admission of fact as the judge considers essential to secure the fairness of the trial of that offence*". There are 3 problems in this provision: 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.

158. 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. They are, with respect, far from being partial at least in the objective sense. 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 and is left to do with whatever information the prosecution is minded to admit, subject only to whatever intervention the judge may wish to make to secure additional or correct admissions.

159. The Bill appears to have adopted the policy of viewing all interceptions of communication as being in the same category as public interest immunity, and in respect of which, should not be disclosed to the persons affected. The law in respect of disclosure of material subject to public interest immunity was discussed by the House of Lords in R v H & Ors [2004] 2 AC 134. Lord Bingham said at paragraph 14:

*14. Fairness ordinarily requires that any material held by the prosecution which weakens its case or strengthens that of the defendant, if not relied on as part of its formal case against the defendant, should be disclosed to the defence. Bitter experience has shown that miscarriages of justice may occur where such material is withheld from disclosure. The golden rule is that full disclosure of such material should be made.*

At paragraph 18:

*18. Circumstances may arise in which material held by the prosecution and tending to undermine the prosecution or assist the defence cannot be disclosed to the defence, fully or even at all, without the risk of serious prejudice to an important public interest….In such circumstances some derogation from the golden rule of full disclosure may be justified but such derogation must always be the minimum derogation necessary to protect the public interest in question and must never imperil the overall fairness of the trial.*

So material must be disclosed unless the prosecutor believes that it should be withheld on the ground of public interest immunity. In that situation he must obtain a judicial ruling.

160. In HKSAR v Chan Kau Tai, (supra), the Hong Kong Court of Appeal applied R v H & Ors (supra) in respect of the disclosure of a witness's previous convictions [paragraph 51]. The Court also applied the Privy Council's judgment in Sinclair v HM Advocate (Devolution) [2005] SLT 563, which held that it is fundamental right to a fair trial that there should be an adversarial procedure in which there is equality of arms between the prosecution and defence [paragraph 63]. The Court held that, "*...the right to material disclosure is an aspect of fair trial. Fair trial as well as equality of arms…are guaranteed by Article 10 of the Hong Kong Bill of Rights and protected by the common law*" [paragraph 64].

161. 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 the restrictions upon obtaining information about prescribed authorizations and products infringe a person's right to a fair trial under the common law, Article 14 of the ICCPR and Article 87 of the Basic Law of the HKSAR, and the right to an "effective remedy" under Article 2(3) of the ICCPR.

162. In Canada, section 189 of the Criminal Code requires the prosecution to give to an accused a transcript of the private communication, and a statement of the time, place and date of the communication and the parties, if known, as well as notice of its intention to produce. Under section 187(1.4), the trial judge has the power to open the "packet" and have the authorization disclosed to the accused, subject to editing: section 187(4). Similar provisions are found in New Zealand in section 312L of the Crimes Act 1961.

163. 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. Without adequate information about the authorization, the execution of the authorization, the obtaining of the product, and the product itself, there is no way that its admission can be effectively challenged. The Administration must also explain what powers a trial judge has to exclude the evidence obtained from any authorizations.

<u>Matters Not Covered by the Bill</u>

164. The Bill has not dealt with the question of the admissibility of an interception or surveillance product which was unlawfully obtained. See, in this connection, the Crimes Act 1961 of New Zealand, section 312M.

165. The Bill has not dealt with the question of whether an interception or surveillance product obtained by a department within the meaning of the Bill pursuant to a prescribed authorization may be made available to another such department, or some other government department such as the Inland Revenue Department, or other regulatory agencies, such as the Securities and Futures Commission. Clause 56 has not explicitly addressed this question.

166. The Bill has not dealt with the question of whether an interception or surveillance product obtained by a department within the meaning of the Bill pursuant to a prescribed authorization may be made available to a law enforcement agency or intelligence/security agency outside Hong Kong's jurisdiction in furtherance of mutual legal assistance or otherwise.

Transitional Arrangements

167. 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.

168. The proposed application of Clause 58 to such materials is inappropriate for the reasons stated above in relation to that clause.

Consequential Amendments

169. Schedule 5 of the Bill contains consequential amendments. The Bar's objections to the proposed consequential amendment to the Telecommunications Ordinance are set out in an earlier part of these Comments under the heading "Interception of Communications".

170. The proposed consequential amendment to the Personal Data (Privacy) Ordinance (Cap 486) purports to grant complete exemption from the requirements of that Ordinance's data protection principles in respect of, inter alia, personal data systems maintained pursuant to Clause 57. Given that the Bar calls for notification to objects of interception of communications or surveillance of the fact of such interception or surveillance, this proposed consequential amendment cannot be accepted.

Dated 24th March 2006.

Hong Kong Bar Association

**Appendix A**

List of Issues for Consultation of Membership

(1) Whether the Bill should bind only public officers as defined in s 3 of the Interpretation and General Clauses Ordinance (Cap 1) or also persons acting on behalf of the HKSAR Government or public officers or further also persons acting on behalf of the State (including subordinate organs of the Central Authorities exercising executive functions in Hong Kong).

(2) Whether the Bill should have specific and adequate provisions affording protection to the professional activities of legal practitioners, and of legal professional privilege. See Clause 2(3) and Schedule 3, Part 1, paragraph (b)(viii); Part 2, paragraph (b)(ix); Part 3, paragraph (b)(ix), for provisions in the Bill making reference to legal professional privileged information.

(3) Whether all forms of interception of communications (inclusive of telecommunications and postal packets) and all forms of covert surveillance (inclusive of surveillance using covertly a recording device, a tracking device, and an optical device, and surveillance by human agents not using any device) should be subject to authorization by a judicial officer.

(4) Whether there should be a statutory provision (Clause 2(2) of the Bill) deeming that a person is not being entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place (which is defined to include all places to which the public have access either continuously or periodically, except public toilets, bathing and changing facilities), with the implication being that surveillance conducted of the person in relation to such activities in a public place so defined is not covert surveillance for the purposes of regulation under the Bill.

(5) Whether it is appropriate to have, as the triggering condition of "prevention or detection of serious crime" for making an authorization of interception of communications or covert surveillance (Clause 3(1)(a)(i)), the following

definition of "serious crime", namely, in respect of interception of communications, offences punishable by not less than 7 years' imprisonment; and in respect of covert surveillance, offences punishable by not less than 3 years' imprisonment (Clause 2(1)).

(6) Whether it is appropriate to have "protection of public security" as a triggering condition for making an authorization of interception of communications or covert surveillance (Clause 3(1)(a)(ii)).

(7) Whether public officers found to have conducted interception of communications or covert surveillance covered by the Bill but without authority pursuant to the Bill should be liable to criminal sanction (Clauses 4, 5).

(8) Whether Court of First Instance judges should be the class of judicial officers eligible to be appointed panel judges to issue judicial authorization for interception of communications and surveillance under the Bill (Clause 6).

(9) Whether panel judges candidates (who are already Court of First Instance judges) should be subject to security clearance before appointment.

(10) Whether panel judges should be appointed by the Chief Executive (Clause 6).

(11) Whether there should be prescribed, as in Schedule 2, paragraph 4 of the Bill, that in performing any of his functions under the Bill, a panel judge shall act judicially and have the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court.

(12) Whether the maximum duration of each judicial authorization (including renewals) should be 3 months (Clauses 10, 13).

(13) Whether it is appropriate for there to be unlimited renewals of judicial authorizations in respect of the same object of interception or surveillance (Clause 12(4)).

(14) Whether the maximum duration of each executive authorization (including renewals) should be 3 months (Clauses 16, 19).

(15) Whether it is appropriate for there to be unlimited renewals of executive authorizations in respect of the same object of surveillance (Clause 18(4)).

(16) Whether the provisions in the Bill for civil immunity of persons for performance or purported performance in good faith of any function, or his compliance with a requirement made or purportedly made, under the provisions in the Bill (namely Clause 61(1)(b) and (c)) are appropriate.

(17) Whether a person who had been an object of interception of communications or covert surveillance should be entitled to be notified that he had been so.

(18) Whether any product of interception of communications or surveillance that was unauthorized should be deemed to be inadmissible or prima facie inadmissible (subject to judicial discretion to admit).

(19) Whether it is appropriate that in criminal proceedings generally any product obtained pursuant to an authorization for interception of communications of telecommunications shall not be admissible in evidence and shall not be made available to any party, and any evidence or question which tends to suggest matters relating to any application for the issue or renewal of that authorization and other related matters shall not be adduced or asked (subject only to specified cases where disclosure is in the interests of justice) (Clause 58).

(20) To what extent should the common law duty of disclosure on the part of the prosecution be modified in the light of the provisions of the Bill.