Comments of the Bar Association
on the Interception of Communications and Surveillance Ordinance (Cap 589)

1. As part of the Administration's Comprehensive Review of the Interception of Communications and Surveillance Ordinance (Cap 589) ("ICSO"), the Government Secretariat, in a letter, dated 28 June 2011, to the Hong Kong Bar Association ("HKBA"), identified areas where the Administration was considering amendments to ICSO, and asked the HKBA to comment.

A. Administration's Proposals

2. The Administration's proposals concern areas identified by the Commissioner on Interception of Communications and Surveillance ("Commissioner") in his Reports to the Chief Executive, which require amendments to ICSO. The HKBA fully supports the Commissioner's recommendations, and has no comments on most areas.

3. However, there are two areas where the HKBA disagrees with the Administration's proposals: first, in relation to the Commissioner being given the power to listen to intercepted communications; and second, the Administration's proposal for the time period within which an interception must be discontinued after the revocation of the prescribed authorization by a panel judge. The HKBA's comments are set out below.

(1) Checking of Intercept Products by the Commissioner

4. The ICSO contains no express power for the Commissioner to listen to recordings of intercepted communications.

5. In para 5.21 of his 2008 Report, the Commissioner referred to the fact that the Administration raised doubts about the legitimacy or propriety of him listening to recordings of intercepted communications in order to ascertain whether the report made by a law enforcement authority ("LEA") to the panel judge on the realization of

the existence of information that is or may be subject of legal professional privilege ("LPP") or journalistic material ("JM"), did or did not contain misrepresentations so as to cause the panel judge to allow the prescribed authorization under which the interception was carried out to continue, instead of revoking it.

6. The Administration drew the Commissioner's attention to the Supreme Court of Canada's decision in *Privacy Commissioner of Canada v Blood Tribe Department of Health and Others,*[1] as authority supporting its view that the Commissioner did not have such power. In that case, the Privacy Commissioner of Canada requested the disclosure of matters that were subject to LPP from one of the parties to the dispute; the party refused - claiming that the matters were subject to LPP. Under the Personal Information Protection and Electronic Documents Act [2] the Privacy Commissioner was in an adversarial relationship with the party being complained about, and wanted the material in order to determine the LPP claim being made by the party. Under the Act the Commissioner had the power to refer the matter to the court for resolution, so there were other means for having the LPP claim resolved.

7. The Supreme Court of Canada held that for the purpose of ensuring compliance with the Act the Privacy Commissioner did not have the express or implicit power to compel the production of material over which LPP was claimed in order to determine an employee's complaint of failure to access personal information.

8. The context in which the LPP issue arose in the *Privacy Commissioner* case and the terms of the Canadian Act are distinguishable from the functions of the Commissioner and terms of ICSO.

9. Denying the Commissioner access to the intercepted material prevents him from fully carrying out his function under ICSO to ensure that it is not being breached or abused in any way.

10. An ordinance may override LPP by express words or necessary implication. In *R (Prudential PLC and Prudential (Gibralter) Limited) v Special Commissioner of*

[1] (2008) SCC 44.
[2] S.C. 2000, c.5.

Income Tax and Another,[3] Mr Justice Charles spoke about Parliament's removal of LPP for the exercise of investigatory powers:

> *(10) An aspect of the proper administration of justice and other functions is the exercise of investigatory powers given to promote the public interests supporting the disclosure of information to assist in the proper performance of those functions....In respect of those powers, the privilege against self-incrimination and the right to claim LPP can be expressly removed, modified or addressed by Parliament and if they are not questions can arise as to whether those rights have been removed or modified by necessary implication.*

11. The meaning of "necessary implication" in the context of LPP was discussed by Lord Hobhouse in *R (Morgan Grenfell & Co Ltd) v Special Commissioner of Income Tax and another*:[4]

> *A necessary implication is not the same as a reasonable implication... A necessary implication is one which necessarily follows from the express provisions of the statute construed in their context. It distinguishes between what it would have been sensible or reasonable for Parliament to have included or what Parliament would, if it had thought about it, probably have included and what it is clear that the express language of the statute shows that the statute must have included. A necessary implication is a matter of express language and logic not interpretation.*

12. The Commissioner's powers to obtain information for carrying out his functions are set out in s.53 of ICSO:

> *53(1) For the purpose of performing any of his functions under this Ordinance, the Commissioner may –*
>
> *(a) require any public officer or any other person to answer any question, and to provide any information, document or other matter in his possession or*

[3] [2009] EWHC 2494 (Admin), para 32.
[4] [2003] 1 AC 563, para 45.

control to the Commissioner, within the time and in the manner specified by the Commissioner when making the requirement; and

(b) require any officer of a department to prepare any report on any case of interception or covert surveillance handled by the department, or on any class of such cases, within the time and in the manner specified by the Commissioner when making the requirement.

....

(3) Notwithstanding any other provision of this Ordinance or any other law, any person on whom a requirement is imposed by the Commissioner under subsection (1) shall comply with the requirement.

13. The HKBA is of the opinion that s.53, by necessary implication, gives the Commissioner the power to obtain from the LEA the intercept products of possible communications that might be covered by LPP or JM and to listen to them.

14. A crucial part of the Commissioner's functions is to ensure that there are no unauthorized interceptions of LPP communications or JM. It is difficult to understand the Administration's argument that he can properly carry out this function without being able to obtain and listen to communications which might show the interception of LPP communications or JM, and whether the panel judge was misled. The Administration's arguments at paras.10-12 of its letter as to why it is not necessary for him to obtain and listen to such matters are unconvincing and do not address the issue. The plain fact is that he cannot properly carry out his functions dependent upon assurances from those whom he has a duty to oversee. In order to satisfy himself that there has been no breach of ICSO, or whether a LEA may have misled a panel judge, the Commissioner must be able to listen to the intercepted communications.

15. If the Administration agrees with the HKBA that the Commissioner has this power by necessary implication, and the Administration undertakes in the future to provide the Commissioner with these intercepted communications to listen to, then there is no need for an amendment. However, if the Administration disagrees with the HKBA, then the HKBA urges the Administration to amend ICSO to give the Commissioner this express power.

16. The HKBA is disappointed that the Administration, relying upon the *Privacy Commissioner* case, appears reluctant to give full support by way of amendment to the ICSO to allow the Commissioner to listen to interceptions that might include LPP communications or JM. Just how the legislation can be amended to give the Commissioner this power, and the restrictions as to the persons acting under the directions of the Commissioner who can listen to the intercepted product, are matters which can be easily resolved.

17. Further, the HKBA reiterates what it said earlier in its comments, dated 20 February 2009, on the Commissioner's 2007 Report: the ICSO and the Code of Practice should make clear that there cannot be any use made of the LLP information, ie to use it as intelligence or otherwise obtain derivative evidence. Further the HKBA strongly recommends that the Code of Practice makes clear that all safeguards are taken so as to ensure that no LPP communications are intercepted, recorded or listened to by LEA's.

(2) Time gap between the revocation of the prescribed authorization and the actual discontinuance of the operation (item (4))

18. The Administration proposes that the LEA must take immediate steps to discontinue the interception or covert surveillance in question, *"as soon as reasonably practicable"*, and proposes that the Code of Practice stipulate a timeframe within which discontinuation should normally be effected.

19. The HKBA does not agree with the Administration's suggested time frame for discontinuance. The Code of Practice is not approved by LegCo, therefore, the Administration is left to decide the appropriate time frame, ie what is meant by *"reasonably practicable"*.

20. The HKBA recommends that the discontinuance be "*immediately*" or *"as soon as possible"*, and that this term be expressly stated in the ICSO.

B. Recommended amendments to ICSO

21. The Administration and Legislative Council should take this valuable opportunity to improve ICSO by amending it in areas where it is deficient or contrary to law. To this end, the HKBA recommends that the following amendments be made to ICSO.

22. A major deficiency of ICSO is that it does not prohibit the unauthorized interception of communications or covert surveillance. Recent events in the UK in the "phone hacking" scandal demonstrate that unauthorized interceptions by private persons bring unimaginable grief to victims.

23. Section 4 of ICSO provides:

> *4. Prohibition on interception*
>
> *(1) Subject to subsection (2), no public officer shall, directly or indirectly (whether through any other person or otherwise), carry out any interception.*
>
> *(2) Subsection (1) does not apply to*
>
> *(a) any interception carried out pursuant to a prescribed authorization;*
>
> *(b) any interception of telecommunications transmitted by radiocommunications (other than the radio-communications part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under the Telecommunications Ordinance (Cap 106); and*
>
> *(c) any interception authorized, permitted or required to be carried out by or under any enactment other than this*

Ordinance (including any interception carried out in the course of the execution of an order of a court authorizing the search of any premises or the seizure of any evidence).

24. Section 4 only refers to "public officer", but does not prohibit private persons from intercepting communications.[5] This is a serious defect in ICSO and leaves victims open to breaches of their privacy right.

25. Section 27(b) of the Telecommunications Ordinance (Cap.106) prohibits a person from damaging, removing or interfering with a telecommunications installation with intent to intercept or discover the contents of a message. This provision does not deal with the act of interception but only the associated act of interference with a telecommunications installation and is therefore limited in scope. Further, s.27A of the Telecommunications Ordinance prohibits a person from knowingly causing, by telecommunications, a computer to perform any function to obtain unauthorized access to any program or data held in a computer. But this provision addresses only one form of computer hacking.

26. In 2006 the Law Reform Commission recommended the creation of criminal offences relating to covert surveillance to prohibit the unlawful obtaining of personal information involving intrusion into private premises. Earlier, in 2004, the Commission recommended the creation of civil liability in tort for a seriously offensive or objectionable intrusion into the privacy of a person. However, in 2009 the Administration announced that it would, "*handle the five reports [of the Commission on privacy] in stages and map out the way forward in consultation with relevant*

[5] There is no definition of "public officer" in ICSO. Section 3 of the Interpretation and General Clauses Ordinance (Cap.1) defines "public officer" to mean "any person holding an office of emolument under the Government, whether such office be permanent or temporary". While both ss. 4 and 5 of ICSO prohibits public officers from carrying out any interception or covert surveillance "directly or indirectly (whether through any other person or otherwise)", it remains to be seen whether the language of these two sections is sufficient to attach criminal liability against public officers who used an "independent contractor" to carry out interception or covert surveillance. The "independent contractor", being not a public officer, is not caught under ss. 4 and 5 directly, and only possibly as an aider or abettor. In any event, it must be pointed out that the carrying out of interception or covert surveillance through "independent contractors" might circumvent the statutory scheme under ICSO of judicial authorization and such circumvention would be difficult to discover or detect.

parties", and the reports containing the recommendations set out above were not the first reports to be taken forward.

27. In contrast, s.184 of the Criminal Code of Canada prohibits any unauthorized interception of communications:

> *184. (1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.*
>
> *(2) Subsection (1) does not apply to*
>
> *(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;*
>
> *(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;*

28. In New Zealand, s.216B(1) of the Crimes Act 1961 states, "*every one is liable to imprisonment for a term not exceeding 2 years who intentionally intercepts any private communication by means of an interception device*". The ensuing sub-sections of s.216B provide that the offence does not apply where: the person intercepting the private communication is a party to that private communication; or does so pursuant to, and in accordance with the terms of statutory authority; to the interception by a constable of a private communication by means of an interception device under prescribed circumstances of emergency; to the monitoring of a prisoner call; and to the interception of private communications by an interception device operated by an internet service provider.

29. In the United Kingdom, s.1 of the Regulation of Investigatory Powers Act 2000 provides for two offences of unlawful interception:

> *1. (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of –*
>
> *(a) a public postal service; or*
>
> *(b) a public telecommunications system.*
>
> *(2) It shall be an offence for a person –*
>
> *(a) intentionally and without lawful authority; and*
>
> *(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,*
>
> *to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.*
>
> *(6) The circumstances in which a person makes an interception of communication in the course of its transmission by means of a private telecommunication are such that his conduct is excluded from criminal liability under subsection (2) if –*
>
> *(a) he is a person with a right to control the operation or the use of the system; or*
>
> *(b) he has the express or implied consent of such a person to make the interception.*

Notification of persons affected

30. There are only two means under ICSO for a person to be notified about whether his communications have been intercepted, or that he has been the subject of covert surveillance. First, under s.43 if a person suspects that he has been the subject of an interception or surveillance, he may apply to the Commissioner for an examination; second, under s.48 the Commissioner may notify a person if he finds that the person has been the subject of an unauthorized interception or surveillance.

31. The ICSO does not provide for the person who has had his communications intercepted or has been the subject of covert surveillance to be notified, as of right, of the interception or surveillance. Therefore, he is unable to pursue any remedy for a possible unauthorized breach of his privacy right.

32. This situation is unacceptable. In the HKBA's Comments on the Interception of Communications and Surveillance Bill, dated 24 March 2006, the HKBA identified this problem and said at para.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 HKBA maintains this position.

33. The right of HKSAR residents to effective remedies for violations of their fundamental rights is guaranteed 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).

34. In *Weber and Saravia v Germany*[6] the European Court of Human Rights ("ECHR") discussed the right of a person whose communications had been intercepted to be notified so that they could to seek an effective remedy:

[6] Application No 54934/00, paras134-135.

> *135. The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively.*

The ECHR recognized that notification could not take place if it would jeopardize an ongoing investigation or could reveal the investigative methods, and found that as soon as notification could be carried out without jeopardizing the purpose of the restriction on notification after the termination of the surveillance measure, information should be provided to the persons concerned.

35. And, in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*,[7] the ECHR found that the Bulgarian surveillance law did not provide sufficient safeguards against the risk of abuse which is inherent in any system of secret surveillance. A matter which the ECHR found lacking in the Bulgarian law was the absence of a requirement for the person affected by the surveillance to be notified of such. It said:

> *91. By contrast, the SSMA does not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time...The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance.*

[7] Application No 62540/00, para 91.

36. Legislation in other jurisdictions provide for notification of persons who have had their communications intercepted. For example, under s.196 of the Criminal Code of Canada, 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, must notify in writing the person who was the object of the interception pursuant to an authorization. Under section 196(2) and (3) of the Code, 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.

37. The HKBA urges the amendment of the ICSO so that persons who have been the subject of authorizations for interception of their communications or covert surveillance are notified as of right, at such time so as to not jeopardize the investigation.

Right of Action for Compensation

38. In para.6.10 of his 2008 Report, the Commissioner described one case where he notified a person pursuant to s.48(1) in respect of the unauthorized interception, and after the person requested him to examine the matter, and upon receiving representations of the person, he made an order under s.44(3) of ICSO for the Government to pay the person $10,000. When performing his functions under ICSO the Commissioner is not regarded as a court of a member of a court: s.55. Therefore, the assessment of compensation is not carried out by a judicial official, and any assessment and order for compensation is not subject to appeal.

39. In contrast, a person who suffers damage by reason of a contravention of a requirement under the Personal Data (Privacy) Ordinance (Cap.486) by a data user relating to his or her personal data is entitled to compensation from that data user for that damage through legal proceedings pursuant to s 66 of that Ordinance.

40. An unauthorized interception of communications or covert surveillance is as much an infringement of a person's personal data privacy, if not more. Accordingly, the HKBA recommends that the ICSO expressly provide that the person have the

right to pursue an action for damages in the courts, to serve as an avenue of redress in addition to having damages assessed by the Commissioner.

"Serious Crime"

41. Section 2(1) of ICSO defines "serious crime" as any offence punishable:

(a) in relation to an authorization for interception, by a maximum penalty that is or includes a term of imprisonment of not less than 7 years;

(b) in relation to an authorization for covert surveillance, by a maximum penalty that is or includes a term or imprisonment of not less than 3 years or a fine of not less than $1 million.

42. The HKBA maintains that the definition of "serious crime" is too wide, and should be narrowed to include only such serious offences where such intrusions of privacy is necessary, such as where the conduct involves the use of violence, results in substantial financial gain, or is conduct by large number of persons in pursuit of a common purpose.

Persons subject to authorizations

43. Section 3(1)(b)(i) of ICSO provides that a prescribed authorization may be granted if there is a, *"reasonable suspicion that any person has been, is, or is likely to be, involved in ....the particular serious crime to be prevented or detected.."* And under (ii), in relation to a threat to public security, the test is that there is a, *"reasonable suspicion that any person has been, is, or is likely to be, involved in...any activity which constitutes or would constitute the particular threat to public security.."*

44. Under Schedule 3, Part 1 of ICSO the affidavit supporting an application for the issue of a judge's authorization for interception, must set out, if known, "*the identity of any person who is the to be the subject of the interception*".

45. The term *"any person"* is not defined, therefore, it may be interpreted to include persons who are not suspected having committed an offence, as opposed to only being involved in a crime – which may be without knowledge or intention. Therefore, an authorization may be made in respect of a person who is not even a suspect of a criminal activity. So long as there is a reasonable suspicion that a person is involved in some sort of criminal activity or threat to public security, other persons who are not involved may be the subject of an authorization.

46. In *Iordachi and Others v Moldova*,[8] the ECHR considered legislation which allowed for interceptions of a *"suspect, defendant or other person involved in a criminal offence"*, and found that the term *"other person involved in a criminal offence"* was not sufficiently clear in the absence of a definition.

47. The HKBA recommends that this situation be clarified by an amendment to ICSO.

Threshold for authorization

48. In s.3(1)(b) of ICSO the threshold for a prescribed authorization is, *"reasonable suspicion that any person has been, is, or is likely to be, involved in..."*

49. Under the Criminal Code of Canada[9] the officer must depose to *"reasonable grounds to believe that an offence...has been or will be committed"*. In New Zealand's Crimes Act 1961,[10] the officer must depose to his *"reasonable grounds for believing that...a person has committed, or is committing, an offence..."*

50. The HKBA's opinion is that the threshold of *"reasonable suspicion"* is too low, and recommends an amendment to bring it in line with the applicable threshold in similar legislation in other jurisdictions, ie *"reasonable grounds for believeing"*.

Other investigative means

[8] Application No 25198/02, para 44.
[9] Section 184.2(2)(a).
[10] Section 312B(1).

51. Section 3(1)(c)(ii) of ICSO provides that a condition for the granting of an authorization is, "*considering whether the purpose sought to be furthered by carrying out the interception or covert surveillance can reasonably be furthered by other less intrusive means*".

52. The HKBA believes that this is inadequate. There is no obligation for a LEA to even attempt to obtain the information by less intrusive means.

53. Similar legislation in other jurisdictions provide for stringent condition to be satisfied before a persons privacy right is interfered with. For example:

(1) In the ECHR judgment in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria,*[11] the condition in the Bulgarian legislation was, "*other methods are deemed unlikely to succeed*".

(2) Section 185(1)(h) of the Criminal Code of Canada requires the applicant to 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: s.186(1)(b) Criminal Code.

(3) Section 312B(1)(e) of New Zealand's Crimes Act 1961 requires the applicant to state that he has "*reasonable grounds to believe*":

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

[11] Application No 62540/00, para 79.

(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: s.312C Crimes Act 1961.

Terms and Conditions

54. Section 29 of ICSO permits the judge or executive to include terms for the better execution of the authorizations.

55. However, ICSO does not contain any express provision for the authorizing judge or to make the authorizations subject to terms and conditions in order to limit the scope of the authorization and to prevent unauthorized interceptions or surveillance. In contrast, under the relevant provisions in the Criminal Code of Canada[12] the authorization issued by the judge must, "*contain such terms and conditions as the judge considers advisable in the public interest*". In New Zealand's

[12] Section 186(4)(d).

Crimes Act 1961[13] the interception warrant must, *"contain such additional terms and conditions as the Judge considers advisable in the public interest."*

56. The HKBA recommends that ICSO be amended to give the judge or authorizing officers the power to include terms and conditions in a prescribed authorization.

Renewals of Authorizations

57. Under s.11 of ICSO an authorization may be renewed, and under subsection (4) the authorization may be renewed more than once. The renewal period can be for up to 3 months: s.13(b).

58. The Commissioner's 2009 Report, Table 1(a) shows that there were 47 authorizations of interception of communications that were renewed during the report period for more than 5 times. Therefore, there are a significant number of authorizations of interception of communications that, by successive renewals, have been in operation for more than 150 days.

59. The same Report shows in Table 1(b) that there were 53 authorizations of surveillance that were renewed during the report period and 3 of those were renewed for more than 5 times. Therefore, there are also authorizations of surveillance that, by successive renewals, have been in operation for more than 60 days.

60. The HKBA is of the opinion that the renewal power is being overused.

Number of authorizations

61. In the Commissioner's 2008 Report, Table 1(a) shows that 801 authorizations were issued, and 13 were refused - only 1.6% of the applications were refused. As well, 918 authorizations were renewed, and 13 renewal applications were refused -

[13] Section 312D(1)(e).

only 1.4% of the renewal applications were refused. Over 2 new authorizations and renewals were issued each day.

62. In the Commissioner's 2009 Report, Table 1(a) shows that 831 authorizations were issued, and 8 applications for authorizations were refused - less than 1% of applications were refused. As well, 950 renewal authorizations were issued, and 7 applications for renewals were refused - only 0.73% of the applications were refused. Over 2 new authorizations and renewals were issued each day.

63. In the HKBA's opinion these figures show alarmingly low rates of refusal, and high numbers of authorizations or renewals. These figures must be viewed put in the context of Hong Kong's low crime rate.

64. In *Iordachi and Others v Moldova*[14] the ECHR considered the number of interception warrants issued under the subject legislation and found that for the 3 years under consideration the application success rate was between 97.93% and 99.24%. The Court observed:

> *51. The Court notes further that in 2007 the Moldovan courts authorized virtually all the requests for interception made by the prosecuting authorities...Since this is an uncommonly high number of authorizations, the Court considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorizing it. The Court notes that the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorizing an interception. Nor does it contain safeguards other than the one provided for in section 6(1), namely that interception should take place only when it is otherwise impossible to achieve the aims. This, in the Court's opinion, is a matter of concern when looked at against the very high percentage of authorizations issued by investigating judges. For the Court, this could reasonably be taken*

[14] Application No 25198/02, para 51.

to indicate that the investigating judges do not address themselves to his existence of compelling justification for authorizing measures of secret surveillance. (emphasis added)

As a result of a number of shortcomings in the Moldovan law, the ECHR considered that it did not provide adequate protection against abuse of power by the State in the field of interception of telephone communications, and therefore, the interference with the applicants' right to privacy was not "in accordance with the law".[15]

65. Although not an exact comparison, in Canada the number of applications for new and renewals for wiretap and video surveillance authorizations made by agents of the Attorney-General of Canada for the years 2007-2010 are set out in the Annual Report on the use of Electronic Surveillance 2010, prepared by the Minister of Public Safety and Emergency Prepardness and presented to Parliament.[16] In New Zealand the Commissioner of Police is required by statute to provide in the annual report presented to Parliament information on the use of interception warrants.[17]

66. In Canada, in 2008 and 2009 there were 80 and 92 applications for wiretap authorizations, respectively. For the same years in New Zealand there were 68 and 99 applications for interception warrants.[18] For the same years in Hong Kong, 801 and 831 intercept authorizations were issued.

67. In Canada in 2008 and 2009, there were 11 and 29 applications, to a judge for video surveillance authorizations, respectively. For the same years in Hong Kong there was a total of 167 authorizations (83 judicial and 84 executive) and 152 authorizations (88 judicial and 64 executive), respectively.

68. In Canada in 2008 and 2009 there were 16 and 10 applications, for renewals of both wiretap and video surveillance authorizations, respectively. In New Zealand

[15] Above, para 53.
[16] Accessible at: http://www.publicsafety.gc.ca/abt/dpr/le/elecsur-10-eng.aspx.
[17] Accessible at: http://www.parliament.nz/NR/rdonlyres/6A9D43E2-AE9C-4C64-9CF5-D402D1CF360D/163076/DBHOH_PAP_20624_NewZealandPoliceNgaPirihimanaOAote.pdf.
[18] The Crimes Act 1961, Part 11A and the Misuse of Drug Act 1975, Part 2 of New Zealand makes no distinction between interception of telecommunications and covert surveillance by means of an interception device.

in 2008 as well as in 2009 there was no application for a renewal of an interception warrant. In Hong Kong in 2008 there were 949 renewals of interception and video surveillance authorizations (918 interception authorizations and 31 video surveillance authorizations; and in 2009 there were 1003 renewals of interception and video surveillance authorizations (950 interception and 53 video surveillance).

69. The HKBA strongly believes that ICSO is being overused, the conditions for the issuance of authorizations are too low, and applications for authorizations and renewals are not being scrutinized by panel judges with the necessary strictness.

Commissioner's Reports

70. Section 49(2) of ICSO sets out the matters that must be included in the Commissioner's Annual Reports to the Chief Executive.

71. The HKBA recommends that s.49(2) be amended to provide for the following matters to be included in the Commissioner's Report.

72. First, Table 2(a) of the Commissioner's 2008 Report sets out the major categories of offences for which prescribed authorizations have been issued or renewed. However, it would be beneficial if the Commissioner identified the following:

(1) The number of authorizations issued or renewed in respect of particular offences. This matter is included in the Report prepared by the Minister of Public Safety under s.195(2)(i) of the Criminal Code of Canada.

(2) The LEA that made applications for authorizations or renewals.

These statistics would provide greater transparency of the use, overuse or abuse by particular LEA's. Similar statistics are included in Table 4 of the Annual Report 2010 of the Canadian Minster of Public Safety.

73. Second, the Report should include:

(1) A breakdown of renewal periods. Presently, s.49(2)(a)(v) provides requires the Report to contain the respective numbers of judge's authorizations and executive authorizations that have been renewed under ICSO during the report period further to 5 or more previous renewals. The Report should set out a breakdown of the renewal periods, ie 30, 60, 90, 120 or more days. This is required under s.195(2)(i) of the Criminal Code of Canada.

(2) The places of interception or surveillance, eg residential, office, or public place. This is required under s.195(2)(j) of the Criminal Code of Canada.

Disclosure to other LEA's in Hong Kong or elsewhere (s 59)

74. The ICSO does not prohibit the transfer of any intercepted or surveillance product, or information about such product, to another LEA or regulatory authority in Hong Kong or elsewhere, including LEAs in Mainland China.

75. Section 59(1) of ICSO provides:

> *(1) Where any protected product has been obtained pursuant to any prescribed authorization issued or renewed under this Ordinance on an application by any officer of a department, the head of the department shall make arrangements to ensure -*
>
> *(a) that the following are limited to the minimum that is necessary for the relevant purpose of the prescribed authorization -*
>
> *(i) the extent to which the protected product is disclosed;*
>
> *(ii) the number of persons to whom any of the protected product is disclosed;*
>
> *(iii) the extent to which the protected product is copied; and*
>
> *(iv) the number of copies made of any of the protected product;*
>
> *(b) that all practicable steps are taken to ensure that the protected product is protected against unauthorized or accidental access, processing, erasure or other use; and*

(c) *that the protected product is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization.*

76. Consequently, under s.59(1)(a) there is nothing to prevent a LEA from disclosing the interception or surveillance product, or information about the product to other LEA's in Hong Kong or overseas for the purposes of their investigations. The Code of Practice issued under ICSO only advises in para.170 that: '*To protect privacy and ensure the integrity of these covert operations, details of each operation should only be made known on a strict "need to know" basis.*' A covert operation in co-operation with another LEA in Hong Kong or elsewhere would lead to transfer and it would be up to the transferee LEA or regulatory authority (the activities of some of which may not be governed by the ICSO or the laws of the HKSAR) to protect the intercepted or surveillance product. This is unacceptable: once the product is disclosed there is no mean by which the LEA can control the unauthorized or accidental access.

Disclosure (s 61)

77. Section 61(4) of ICSO provides for the disclosure of information obtained pursuant to a prescribed authorization to be disclosed to the prosecution. Subsections (4) to (6) read:

(4) *Notwithstanding subsection (2) or any other provision of this Ordinance, where, for the purposes of any criminal proceedings (whether being criminal proceedings (whether being criminal proceedings instituted for an offence or any related proceedings), any information obtained pursuant to a relevant prescribed authorization and continuing to be available to the department concerned might reasonably be considered capable of undermining the case for the prosecution against the defence or of assisting the case for the defence -*

(a) *the department shall disclose the information to the prosecution; and*

(b) the prosecution shall then disclose the information to the judge in an ex parte hearing that is held in private.

(5) The judge may, further to the disclosure to him of the information under subsection (4)(b), make such orders as he thinks fit for the purpose of securing the fairness of the proceedings.

(6) Where any order is made under subsection (5) in any criminal proceedings, the prosecution shall disclose to the judge for any related proceedings the terms of the order and the information concerned in an ex parte hearing that is held in private.

78. The wording in ss.(4), "*might reasonably considered capable of undermining the case for the prosecution against the defence or assisting the case for the defence*", is similar to s.3 of the UK's Criminal Procedure and Investigations Act 1996, which sets out the obligation of disclosure by the prosecution to the defence.

79. The principle of disclosure was discussed by Lord Bingham in *R v H and C*[19] that:-

> *Fairness ordinarily requires that any material held by the prosecution which weakens its case or strengthens that of 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.*

80. Disclosable material includes anything available to the prosecution which may undermine confidence in the accuracy of evidence called by the prosecution, or which may provide a measure of support for the defence at trial.[20]

81. The provisions for disclosure in ss.(4) of ICSO do not comply with the disclosure law under common law, or under Article 39 of the Basic Law or Article 11(2) of the Hong Kong Bill of Rights Ordinance (Cap 383), for the following reasons.

---

[19] [2004] 2 AC 134, para 14.
[20] *R v Barkshire and Others,* Court of Appeal (Criminal Division,) 20 July 2011, para 9.

82. First, the LEA is left to decided whether the information is disclosable. However, the LEA which obtained the information should not be deciding whether the information is disclosable to the prosecution: they are not learned about disclosure, and are not responsible, nor have the duty for disclosure – that is the prosecution's duty. Further, LEA's would not have any idea of what the defence case might possibly be. Therefore, they cannot be left to decide for themselves whether the information might undermine the prosecution case or assist the defence. If the LEA decides not to pass the information to the prosecution then there is no means by which the defendant will ever know about it.

To ensure that the LEA provides the information to the prosecution, the ICSO should be amended to make it the duty of the prosecution to review the information. This is the duty of the prosecution: in the Court of Final Appeal case of *Hall v HKSAR*,[21] Mr Justice Bokhary PJ said:

> *The prosecution's duty to disclose relevant material is preceded by a duty to "ascertain" what relevant material exists"*

83. Second, disclosure to a judge occurs rarely where the disclosable material might be the subject of public interest immunity so an *ex parte* hearing is held to prevent the otherwise disclosable for material from being disclosed directly to the defence. In all other case the material is disclosed to the defence as of right. Since the *ex parte* hearing is held in private between just the judge and the prosecutor there is no one to speak on behalf of the defendant. The judge will not know what the defence is, so he cannot make an informed decision.

Therefore, the ICSO should be amended to require the prosecution to disclose all disclosable information directly to the defendant.

Dated 9th September 2011.

Hong Kong Bar Association

---

[21] [2009] 6 HKC 15, para 3.