



Interception of Communications and Surveillance Bill Submission of the Law Society of Hong Kong on other aspects of the Bill

Introduction

The Law Society has made its submission on the issue of legal professional privilege on 12 May 2006. The Law Society has also reviewed various documents tabled before the Bills Committee of the Legislative Council, including in particular the following documents:

- ♦ Submissions from the Bar Association dated 24 March 2006, and the Bar Association's supplementary submission dated 6 April 2006
- ♦ Submission from the Privacy Commissioner for Personal Data dated 28 March 2006
- ♦ The Administration's papers in response to various issues raised
- ♦ The Law Reform Commission's Report "*Privacy: the regulation of covert surveillance*" published in March 2006

Rather than repeating the comments raised in other parties' submissions, the Law Society will endorse the submissions with which it concurs, and put forward additional commentary where appropriate.

The Law Society does not consider this submission to be exhaustive. It reserves the right to make further comments where appropriate.

Legend

Bar = The Hong Kong Bar Association

PCO = Privacy Commissioner for Personal Data

LRC = The Law Reform Commission of Hong Kong

LPP = Legal Professional Privilege

LEA = Law Enforcement Agency

CFI = Court of First Instance

PROVISIONS IN THE BILL AND SUBMISSIONS FROM OTHER PARTIES	THE LAW SOCIETY’S VIEWS
1. Covert Surveillance: Activities in Public Places	
<p>Bill: Clause 2(2) stipulates that a person is not entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place.</p> <p>The Bar’s submission: “Clause 2(2) is based on 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.” (paras. 40-46)</p>	<p>In the Administration’s response to the Bar’s submission, it was pointed out that Clause 2(2) only applies to “<i>activity</i>” carried out in a public place, in distinction to the term “<i>words spoken</i>” used in the Bill. However, the Law Society notes that there is no definition of the word “<i>activity</i>” under the Bill and considers that it is not clear from the Bill that “<i>activity</i>” does not cover conversations. This must be made clear by inserting a suitable definition clause.</p> <p>Putting aside the drafting issue mentioned above, the Law Society submits that as a matter of principle it is not right to define in local legislation that one can never have an expectation of privacy in a public place. International jurisprudence shows that whether one’s activity (whether by way of conversation or act) is carried out in a public place is just one of the factors to</p>

be considered by the court for deciding whether one has a reasonable expectation of privacy. In particular, the definition of “*public place*” could include a restaurant and even a private room in a restaurant, where one would have an expectation of privacy. Hence, excluding all activities carried out in a public place from the operation of the Bill contravene the rights guaranteed in the ICCPR and Article 39 of the Basic Law.

2. Type 2 surveillance: participant-monitoring surveillance

The Bar’s submission:

“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.” (para. 29)

1. The Law Society shares the Bar’s reservations that participant-monitoring surveillance would not require judicial authorization.
2. Case law suggests there is still an intrusion on the privacy of a person even where undercover agents use covert surveillance devices. (see e.g. The Canadian Supreme Court's decision in *R v Duarte* [1990] 1 SCR 90, as discussed in the LRC Report paras 2.18-2.24). Notwithstanding that a person intends to communicate orally to another, he should still have a legitimate expectation of privacy that the conversation would not be covertly recorded by the other person as an agent for an LEA. Moreover, participant-monitoring by undercover agents may intrude upon an accused's right to silence (i.e. an accused has a right to choose whether to answer questions from the LEAs upon being cautioned). The likely infringement of this right is an important factor that should be taken into account by the authorizing judge in carrying out the proportionality

	<p>test. By-passing judicial authorization for all participant-monitoring may allow the LEAs to circumvent an accused's right to silence and their corresponding duty to caution an accused before soliciting information from him.</p> <p>3. The Law Society remains unconvinced by the Administration's argument that the degree of intrusion in participant-monitoring is less than that required for Type 1 surveillance and so does not require judicial authorization, and invites it to clarify its stance.</p>
<p>3. Conditions for Prescribed Authorization: Public Security and Serious Crime</p>	
<p>Bill: In Clause 3(1)(a), the two legitimate purposes for obtaining a prescribed authorization are:</p> <ul style="list-style-type: none"> i. Preventing or detecting serious crime; or ii. Protecting public security. <p>In Clause 2(1), "<i>serious crime</i>" is defined to include offences punishable by over 7 years' imprisonment (for interception of communications) and 3 years' imprisonment (for covert surveillance).</p> <p>No definition of "<i>public security</i>" is given in the Bill.</p> <p>The Bar's submission:</p>	<p>1. The Law Society agrees with the Bar that the term "<i>public security</i>" is vague and should be left out of the Bill, unless a clear definition is inserted.</p> <p>2. The Administration has given some examples of non-crime "<i>public security</i>" cases in its recent paper and has suggested the adoption of an exclusion clause "in connection with (a) external events that have no relevance to our public security and (b) peaceful advocacy, protest or dissent" (SB Ref: ICSB 5/06). The Law Society remains unconvinced by the Administration's clarification and suggestion.</p> <p>3. The Law Society notes the "non-crime" examples cited by the</p>

Para. 65: “It is advisable to leave of the Bill the concept of ‘public security’.” (para. 65)

Administration are concerned primarily with international criminal conduct which do not constitute an offence committed in Hong Kong but which justify interception of covert surveillance so as to help the HK Government discharge its obligations towards the international community for combating crime. The Law Society notes the need to enable covert operations to be conducted by the LEAs in the examples given, but does not accept that the solution lies in including the vague concept of “*public security*” in the Bill. The Law Society considers that the problems envisaged by the Administration arise because the acts do not constitute an offence committed in Hong Kong. However, such problems could be solved by adding a deeming provision in the Bill to the effect that “serious crimes” include acts committed or to be committed outside Hong Kong, which would have constituted a serious offence in Hong Kong had the acts taken place inside Hong Kong (c.f. similar formulae adopted in extradition agreements / statutes). By adopting this approach the Administration can avoid the concerns expressed on the vague phrase “*public security*”.

4. As regards the suggestion of an exclusion clause, it is submitted that this does not provide a satisfactory solution to the problem. Without a clear definition and statutory guidance, the authorizing authority would have great difficulty in coming up with a proper and consistent approach as to what constitutes “*public security*” in the context of the Bill. One must

	<p>bear in mind that the matter needs to be decided on an ex-parte and urgent basis, so that the authorizing authority would have no time to do any research or in-depth study on the international jurisprudence and is not assisted by opposing arguments. The matter is further aggravated in cases of Type 2 surveillance where only internal executive authorization is needed.</p>
<p>4. Conditions for Prescribed Authorization: Threshold for findings</p>	
<p>The Bar’s submission: “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.” (para. 66)</p>	<ol style="list-style-type: none"> 1. Without any threshold being set, an aggrieved party would have no recourse to any sanctions. A threshold should be set as the proposal envisages authorization being granted by a CFI judge. 2. In relation to search warrants, magistrates often have a very wide discretion; the threshold test for prescribed authorizations must be proportionate. 3. The applicant must provide “reasonable grounds” on oath in support of the application.
<p>5. Conditions for Prescribed Authorizations: the Proportionality Test</p>	
<p>Bill: Clause 3(1)(b) provides a test of proportionality, which includes, in subparagraph (i): “<i>balancing, in operational terms,</i></p>	<ol style="list-style-type: none"> 1. We support the submissions by the Bar and the PCO and submit the reference to “<i>in operational terms</i>” should be deleted.

the relevant factors against the intrusiveness of the interception or covert surveillance on any person who is to be the subject of or may be affected by the interception or covert surveillance”.

Other submissions:

PCO’s submission (para. III)

The Bar’s submission (para. 67069)

LRC Report (paras. 3.16-3.22)

The Bar and PCO submit that the term “*operational terms*” is too wide and should be deleted.

2. The Administration has recently explained the inclusion of this reference is to ensure that the authorizing authority does not consider the application in isolation, but as part of an overall operation. The Law Society submits the inclusion of the phrase “*in operational terms*” may not reflect such an intention and may be interpreted differently. The Administration’s intention would be better reflected by using the phrase “*balancing, in the context of the overall operation, the relevant factors ...*”.
3. The Law Society further submits that balancing the relevant factors against only the “*the intrusiveness of the interception or covert surveillance ...*” is too narrow. Apart from the intrusiveness, other fundamental rights may also be at stake, e.g. the right to LPP and the right to silence. The Law Society therefore suggests that the balancing exercise should also cover “*other rights and obligations that may likely be infringed*”.
4. LRC’s test should be adopted, namely: “*there is reasonable suspicion that an individual is committing, has committed, or is about to commit, a serious crime, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong*” (para. 3.21(a) of the LRC Report).

5. The 14 items listed in paragraph 4.4 of the LRC Report should be specifically included in an application for a prescribed authorization:
 - a. *The name and rank or post of the person making the application;*
 - b. *The ground(s) upon which a warrant or internal authorization is sought;*
 - c. *The facts relied upon to justify the belief that a warrant or internal authorization should be issued, including the particulars of the crime, including serious crime under investigation, or the threat to public security in respect of Hong Kong;*
 - d. *The identity of the individual(s), if known, who is or are to be the subject of the covert surveillance;*
 - e. *The information sought through covert surveillance;*
 - f. *The form of covert surveillance and the kind of surveillance device(s) to be used;*
 - g. *The location of the facilities from which, or the place where, the covert surveillance is to be carried out;*
 - h. *The number of instances, if any, on which an application for a warrant or internal authorization has been made in relation to the same subject matter or the same person and whether that previous application was rejected or withdrawn;*
 - i. *The period for which the warrant or authorization is requested;*
 - j. *Whether the covert surveillance is likely to result in any person acquiring knowledge of matters subject to legal privilege, confidential journalistic*

	<p><i>information or sensitive personal information;</i></p> <p><i>k. The details of any potential collateral intrusion and why the intrusion is justified;</i></p> <p><i>l. Whether other less intrusive means have been tried and why they have failed or are unlikely to succeed;</i></p> <p><i>m. The reasons why the covert surveillance is considered proportionate to what it seeks to achieve; and</i></p> <p><i>n. The extent of which, and the number of persons to whom, any material obtained by covert surveillance is likely to be disclosed; the extent to which the surveillance material will be copied and the estimated number of copies likely to be made of any of the surveillance material obtained.</i></p>
<p>6. Panel Judges and Security Clearance</p>	
<p>The Bar’s submission:</p> <p>“Clause 6 proposes that ‘judicial authorization’ of interception of communications and Type 1 surveillance will be undertaken by panel judges (who are CFI judges) appointed by the Chief Executive upon recommendation by the Chief Justice.” (para. 87)</p> <p>“The scheme of authorization proposed for interception of communications and Type 1 surveillance is one of <u>executive authorization by judges</u>” (para. 92)</p> <p>“The wording of Schedule 2, paragraph 4 of the Bill is</p>	<ol style="list-style-type: none"> 1. There are legal, practical and operational objections to the proposals for panel judges and security clearance. 2. The Panel judges would be dealing with administrative applications virtually on a full time basis and so they would be acting administratively rather than judicially. Reviewing such applications is tedious work and the prospect of being appointed to the Panel could affect recruitment of candidates for appointment to the High Court. 3. As the regulatory scheme needs a mature authorizing body, District Court

problematic from the perspective of separation of powers....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 information judicial power....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." (paras. 97-98)

"The Administration has not put forward a case to justify the imposition of the highest level of integrity checking upon panel judges and candidates." (para. 43)

judges should be excluded. Authorization can only be provided by appointed CFI judges. In order to prevent the creation of two tiers of CFI judges this scheme should apply to all CFI judges. The creation of a specialized panel could encourage the view that certain judges are "prosecution-minded".

4. It is inappropriate for the CE to make appointments to the Panel as there should be a clear separation of functions between the Executive and the Judiciary. The proposed arrangement is a violation of the principle of the separation of powers established under the Basic Law
5. The additional security clearance for panel judges will set a bad precedent. The Administration's failure to provide any criteria for selection is unacceptable as ultimately appointment will be an Executive decision. Currently, all CFI judges have the authority to deal with very sensitive material, including those involving national security. **If a judge fails the proposed security check, would that judge still be able to hear sensitive material in other cases?**

7. Applying for Judicial Authorization

The Bar's submission:

“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.” (para. 106)

“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....The information and fact sought to be asserted before the panel judge must be fully particularized and meet a high threshold of assurance.” (para. 110)

The Bar's views are endorsed. The information and the facts sought to be asserted before a judge must be fully particularized and meet a high threshold of assurance. The deponent must provide “*reasonable grounds as to belief*” in the affidavit.

The deponent should support the application by particulars and indicate whether the informant has provided reliable information in the past. The identity of informants must be protected and should be handed to the judge in a sealed envelope.

8. Determining an Application for Judicial Authorization

Bill:

Clause 9 states that the panel judge may issue the judicial authorization “*with or without variations*”.

Clause 31 states that an authorization may be issued subject to any conditions specified in it that apply to the authorization

The Law Society agrees with the Bar's comments that there should be provisions requiring a judge to consider and formulate the terms of his authorization to minimize the interference with the right to privacy. Any authorization should be for a minimum period with minimum interference.

itself.

The Bar’s submission:

“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.” (para. 115)

9. Duration and Renewal of Judicial Authorization

Bill:

Judicial authorizations or renewals are effective for 3 months (Clause 10(b), 13(b)).

Under Clause 12, a judicial authorization may be renewed more than once so long as “*the conditions for its grant under section 3 have been met*”.

The Bar’s submission:

“The Administration must justify the 3 month period of authorization proposed in the Bill” (para. 119)

1. There should not be a blanket 3-month period. The onus should be on the LEAs to justify any authorization for this length of time. The basis for any authorization should be “*the minimum necessary*” as the judge has a duty to minimize intrusion into the privacy of the suspect. The authorizing judge should not act as a “rubber stamp” and should consider factors such as the aggregate amount of time and the need for more information.
2. Over the course of an investigation, the extent of the intrusion may change. When a suspect does not have any knowledge of the LEAs’ interception, his behaviour will be different compared to the behaviour should he be arrested. If the target has been brought in for enquiries or arrested, it is more likely that the surveillance / interception may intrude upon other rights, such as the right to silence and LPP communication

	<p>with his lawyers.</p> <ol style="list-style-type: none"> 3. The Law Society believes that the initial authorization should end at the time when the suspect is alerted to the investigations (i.e. upon arrest or contact by the LEAs). If the LEAs wish to continue to intercept communications of the suspect, they need to seek fresh authorization. 4. Renewals of applications should not be automatic. When applying for an extension, there must be a full disclosure of all the relevant information by the judge, including the likelihood of interception of conversations subject to legal professional privilege. The LEAs must cite any additional grounds.
<p>10. Executive Authorizations</p>	
<p>The Bar’s submission: “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.” (para. 125)</p>	<ol style="list-style-type: none"> 1. There is a duty to minimize any intrusion of the target’s privacy. The aggregate period should not exceed the maximum period permitted under the 1st authorization; once the aggregate period has been reached there must be a new application to extend the authorization. 2. If a suspect has been arrested he has a right to remain silent and once this right is in place there should be a statutory requirement for additional authorization of continued interception.

	<p>3. A judge should authorize all renewals. The Administration must explain why it proposes applications for renewals of executive authorizations should not be subjected to external review.</p>
<p>11. “Also” and “Further” Authorizations</p>	
<p>The Bar’s submission (Paras. 126-130)</p>	<p>The Law Society submits there should not be any “<i>deeming provisions</i>”.</p>
<p>12. Sanctions for Abuse</p>	
<p>Bill: Clause 61 provides immunity from civil or criminal liability for a number of situations.</p> <p>The Bar’s submission: “The immunity provisions in Clause 61 appear to be too wide. Only Clause 61(1)(a) alone is acceptable.” (para. 140)</p> <p>“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.” (para. 84)</p> <p>“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</p>	<ol style="list-style-type: none"> 1. Clause 61(1)(b) provides that a person shall not incur any civil or criminal liability if he has acted in good faith, which means presumably that immunity from suit should not be applicable when the LEA has acted in bad faith. 2. In the recent judgment of <i>Watkins v. Home Office and others</i> [2006] UKHL 17, the House of Lords considered the issue of civil liability in the tort of misfeasance in public office for intercepting correspondence with legal advisers and courts by public officers. At trial, it was established that a number of prison staff had acted in bad faith by opening and reading material protected by LPP in breach of the Prison Rules when they were not entitled to do so. The House of Lords held that even though it was unlawful for the prison staff to interfere with the appellant’s enjoyment of his right to confidential legal correspondence, he could not succeed in his civil action in tort for misfeasance in public office as he

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)” (para. 86)

had suffered no “material damage” (i.e. financial loss, or physical or mental injury).

3. In the light of *Watkins*, the Bill fails to provide adequate safeguard for breach of LPP by public officers who have intercepted LPP material in bad faith, or maliciously or recklessly. A private individual whose right to LPP has been infringed will not have a civil remedy in tort in the absence of proof of any material damage. The public law remedies will be illusory.
4. In order to address *Watkins*, the Bill should specifically provide for the creation of a statutory duty on the part of any public officer to respect privacy in general, and observe LPP in particular; any breach of such statutory duty, if not in good faith, would give rise to both criminal proceedings and a civil remedy in damages against that public officer by the individuals whose rights have been infringed, without the necessity of proof of “material damage”.
5. The Administration has put forward the argument that it would be wrong to impose criminal sanctions on LEAs when private individuals can intercept communications. It should be noted that the LEAs have significant resources and intrusion by LEAs would not be on the same scale as individuals. The unlawful intrusion onto property can be

	<p>quantified but intrusion into communications cannot. The proposed regulatory scheme is an authorization to intrude into a person’s basic rights. Intrusions into privacy are so great that LEAs should be criminally sanctioned for any abuse, and it should not be left to internal disciplinary action as put forward by the Administration.</p> <p>6. The current proposal fails to impose proportionate checks and balances. It should be noted that under the Banking Ordinance and the Securities and Futures Ordinance, similar offences can carry a maximum fine of \$1 million and a maximum term of imprisonment of 2 years (s.120 of the Banking Ordinance and s.378 of the Securities and Futures Ordinance).</p> <p>7. Two separate criminal offences should be created for:</p> <ul style="list-style-type: none"> (i) unauthorized covert surveillance; and (ii) dealing with protected products in an improper manner (e.g. disclosure of protected products to third parties). <p>8. The appropriate threshold should be “<i>deliberately</i>” or “<i>recklessly</i>”.</p>
<p>13. Notification given to data subjects</p>	
<p>Submissions of other parties:</p> <ul style="list-style-type: none"> ♦ PCO’s submission (para. IV) ♦ The LRC Report (para. 7.11-7.15) 	<p>An intercepted target should be notified of the covert operation unless it will jeopardize the operation or investigation.</p>

<p>♦ The Bar’s submission: “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. 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.” (paras. 136-137)</p>	<p>When notification is provided, there should be sufficient details to enable the target to decide whether or not he should seek compensation (LRC Report para. 7.15). The target should also be allowed access to the application documents (save and except those sensitive parts where the LEAs can legitimately claim public interest immunity).</p>
<p>14. Data subject stripped of his data access request rights</p>	
<p>PCO’s submission (para. IX)</p>	<p>The Law Society agrees with the PCO that Clause 45(2) which grants outright denial of access of personal data is unnecessary.</p>
<p>15. The Commissioner on Interception of Communications and Surveillance</p>	
<p>The Bar’s submission: “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.” (para. 61)</p>	<ol style="list-style-type: none"> 1. The Commissioner should be a retired High Court Judge or above. 2. Clause 47 does not provide the Commissioner with any investigatory powers. The Law Society adopts the LRC’s recommendation that the Commissioner should have the authority to investigate whether the original authorization was validly granted (para. 8.7 of the LRC Report).

<p>“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 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.” (para. 142)</p> <p>“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. 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.” (para. 147)</p>	<ol style="list-style-type: none"> 3. The Bar suggests the Commissioner should not be “<i>constrained in his examination functions by the straitjacket of principles applicable to judicial review</i>” whilst the LRC recommends JR procedures. It should be noted that the scope of judicial review is constantly evolving, especially when fundamental rights are involved. The Law Society supports the Bar’s position. 4. The Report to the Chief Executive should be comprehensive and the provisions in the Bill, as drafted, are inadequate. The Law Society endorses the Bar’s position on the Commissioner’s Report to the CE.
<p>16. Effective Remedies</p>	
<p>Submissions of other parties: PCO’s submission (para. VIII) LRC Report (paras. 8.34-8.38)</p>	<ol style="list-style-type: none"> 1. Under the Bill, there is no formal mechanism to enable an aggrieved person to discover unauthorized intrusion into his privacy. There should be a positive duty to notify as soon as it does not compromise the

<p>The Bar’s submission:</p> <p>“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 surveillance.” (para. 150)</p>	<p>investigation.</p> <ol style="list-style-type: none"> 2. The remedies should be in line with the LRC recommendations. 3. Concern has been raised that without a statutory right of appeal to the Court of Appeal, decisions made by the Commissioner cannot be challenged, and the complainant’s rights would become illusory. There should be provisions in the Bill providing for a right of appeal and the relevant procedures, to enable such a right to be pursued.
<p>17. Code of Practice</p>	
<p>Submission of other parties:</p> <ul style="list-style-type: none"> ♦ PCO’s submission (para. VIII) ♦ The Bar’s submission: <p>“The Code of Practice should be laid before the Legislative Council....[It] should address similar issues addressed in the codes of practice in the United Kingdom so that:</p> <ol style="list-style-type: none"> (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 	<p>The views of the PCO and the Bar are endorsed. The Code of Practice must be introduced as subsidiary legislation.</p>

under the legislation.”
(para. 151)

18. Disclosure

The Bar’s submission:

“There is a strong body of opinion among the experienced members practicing 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.” (para. 153)

The Law Society agrees with the Bar that the defence in criminal proceedings should have access to the intercepted materials and be able to produce them as evidence solely for the purpose of the defence. In addition, there should be a duty to retain all unused materials until the conclusion of all proceedings including appeals.

Council
The Law Society of Hong Kong
16 May 2006

96534 v3