

香港人權監察
HONG KONG HUMAN RIGHTS MONITOR

香港上環孖沙街二十號金德樓4樓

4/F Kam Tak Building, 20 Mercer Street, Sheung Wan, Hong Kong

電話 Phone: (852) 2811-4488 傳真 Fax: (852) 2802-6012

電郵地址 Email: contact@hkhrm.org.hk 網址 Website: <http://www.hkhrm.org.hk>

**The Legislative Council of
The Hong Kong Special Administrative Region
Bills Committee on Interception of Communications & Surveillance Bill**

Submission By Hong Kong Human Rights Monitor

3rd April 2006

Introduction

1. Hong Kong Human Rights Monitor (the Monitor) submits that any legislation on this front has to conform with the rights as guaranteed in the International Covenant on Civil and Political Rights (ICCPR). The Monitor reiterates that Article 30 of the Basic Law should be interpreted and applied in a way which offers no less protection as afforded by the ICCPR.
2. Article 30 of the Basic Law stipulates that "The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may on any grounds, infringe upon the freedom and privacy of communication of residents. Exceptions are provided where "relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences".
3. The Monitor submits that any local legislation providing for such exceptions, such as those in the current Bill, should have the exceptions defined and provided for in a strictly narrow sense and

satisfy all the requirements in the "prescribed by the law" test¹.

4. In spite of being on notice for many years of the importance to pass such legislation, it was not until recent court cases which ruled these activities to be unconstitutional that the government was pushed into action. The unjustified refusal of the HKSAR Government to act and the defeat of the Government in court cases on the legal basis of interception of communications and covert surveillance have left Hong Kong with little time to enact the law.²
5. The Monitor is concerned over the lack of time (6 months) in total to scrutinize the bill. The Monitor cautiously welcomes the introduction of such a law on the basis that "something is better than nothing". It remains concerned that to speed up the enactment of the Bill to empower and regulate the HKSAR Government and their agent's acts in the interception of communications and covert surveillance, the scope of the legislation, for the time being, has to be restricted to the HKSAR authorities only. Intrusion of privacy by the private actors are not covered.
6. The right to privacy should also be protected against violations both by the government and public authorities as well as private individuals. They should be dealt with properly in future legislation.
7. Even with the best efforts by all parties concerned, there may be defects which have been overlooked as a result of the tremendous time pressure. It is therefore advisable to have a sunset clause for the Ordinance which is enacted in haste to allow for a scheduled systematic review and amendments of the Ordinance in the reasonable future to rectify any defects.
8. The Monitor remains concerned that the Government may seek another interpretation of the Basic Law from the Standing Committee of the National People's Congress to resurrect the Executive Order issued by the Chief Executive and to save Section 33 of the Telecommunications Ordinance if the legislation is not

¹ See the Court of Final Appeal's ruling on Leung Kwok Hung's case.

² Laws on surveillance are long overdue, SCMP, 10 Feb 2006.

enacted in time for whatever reasons and if the court does not agree to or is found not to have any power to any extend the grace period. We urge the HKSAR Government to openly commit to not resorting to any interpretation of the Basic Law on this issue.³

Panel Judges

9. The Monitor is concerned over the so-called “integrity checks” which would be used to vet judges who will be on the panel of judges which will be authorizing interception and surveillance applications.
10. The Monitor is of the view that this sort of vetting could open up potential political background checks or could lead to abuse of information to pressurize members of the judiciary. We have great reservation on such vetting. Such integrity checks could be an excuse to filter out judges critical of the Government or law enforcement authorities. This could have an adverse impact to the independence of the judiciary.
11. The Monitor submits that judges in accordance with established principles should be allowed to have ‘security of tenure’, and having in Section 6(2), an appointment of 3 years, could adversely affect the independence of the judges and the public perception of such independence. Worst of all, any appointment system allows the Government to not to appoint or renew the terms of judges who are more critical of the government or law enforcement authorities.
12. To address these concerns, the selection of High Court judges for judicial authorisation should be left entirely to the judiciary.
13. While the Monitor is happy that High Court judges are allowed to authorise the more intrusive acts, it believes that all other less intrusive ones should still be authorised judicially unless cogently justified by the Administration in accordance with international human rights standards. The Legislative Council and the Administration should explore whether it is possible to have

³ Laws on surveillance are long overdue, SCMP, 10 Feb 2006.

District Court judges to take up the authorisation or post act rectification over less intrusive acts. This will provide better independent authorisation of at least some of the less intrusive ones, leaving only those really strictly justified, if any, to very senior law enforcement officers. It is for the Administration to prove with cogent evidence that there should still be exceptions left to be authorised by senior law enforcement officers.

Types of Surveillance

14. The types of surveillance are divided into Types 1 and 2. Type 2 surveillance is under the proposed section 2 set out to mean any “covert surveillance” – meaning “any systematic surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation if the surveillance, is carried out in circumstances where any person who is the subject of covert surveillance is entitled to a reasonable expectation of privacy”, the Monitor submits that this reasonable expectation of privacy begs for a definition, since this reasonable expectation could be construed in different ways by front line as opposed to authorizing officers.
15. The Monitor is concerned over the “executive authorization” which is provided for in Section 14 of the bill, since the application is merely “supported by a statement in writing” made by the applicant giving it no assurance of reliability.
16. Section 2 (b) under Type 2 Surveillance sets out that “...the use of the device does not involve entry onto any premises without permission”, The Monitor however is unsure whether this encompasses seeking permission to intercept communications or conduct surveillance. There are many grey areas such as to who this permission should come from, and whether it should come from the target person (e.g. in a hotel or hostel scenario etc.)

Concepts of “Public Security” and “Serious Crime”

17. The Monitor finds the term in the proposed Section 3 of the bill referring to ““public security” is a concept which is too vague for the purposes of authorising acts which are intrusive to privacy by law enforcement agencies.
18. Under Section 3(2)(a)(ii), the relevant factors to be taken into consideration once again include “serious crime to be prevented or detected or the particular threat to public security”, the Monitor submits that these definitions should be as mentioned, set out in a clear manner, there is no room for ambiguity in such a contentious area.
19. This concept, unless clearly and narrowly defined, could potentially be used to authorise unjustified acts of interception or surveillance. The Monitor submits that the concept should be defined and be confined in a strict, if not stricter, manner.
20. The Police Force Ordinance empowers and obliges the police to prevent and detect crimes. It however does not confer upon the police any political roles or does it empower it to conduct any political surveillance. It allows no jurisdiction for the police on "public security" matters except in cases to "prevent and detect crimes" which are already provided for in the Police Force Ordinance. So are the legal situations of other law enforcement agencies. No law enforcement agency in Hong Kong should be turned into a political tool. The Government, LegCo, the civil society and the public should prevent the forcing or allowing of the police and other law enforcement agencies to take up any political roles intentionally or inadvertently through the provisions of the Bill.
21. In light of existing Ordinances such as the Police Force one, the concept of "public security" should be seen as crime prevention and detection related. We submit that such acts on "security" grounds should be confined to e.g. prevention and detection of the offences of terrorist activities, following the enactment of anti-terrorist legislation in recent years. We also call for the narrowing down of the concept of terrorist acts and providing more safeguards into Hong Kong's anti-terrorism laws such as the United Nations (Anti-Terrorism Measures) Ordinance.

22. Criminal offences to outlaw any act of interception and surveillance for political purpose is necessary to prevent them from becoming political tools and to protect integrity of the police force and other law enforcement agencies and their officers from any political pressure.
23. The Monitor is seriously concerned about the murky history of Hong Kong in relation to conducting surveillance of groups and individuals for political reasons. Political interception and surveillance should not be allowed under the current Bill, and they should be expressly prohibited and any contravention should be criminalized. We urge the Government and LegCo Members to introduce such amendments to the current Bill. Moreover, the power of the Chief Executive to direct the police force under Section 4 of the Police Forces⁴ Ordinance should be either abolished totally to guarantee the neutrality of the police or expressly qualify and subject it to the restrictions of the current Bill.

Presumption

24. The proposed Section 2(2) introduces the presumption that “a person is not regarded as being entitled to a reasonable expectation of privacy ... in relation to any activity carried out by him in a public place” with limited exclusion. This presumption is an unjustified assumption without giving due regard to the fact that many activities a person carries out in a public place still often carries some expectation of privacy. The Monitor submits that this is against the constitutional right to privacy set out under Article 30 of the Basic Law and protected by the ICCPR. Moreover, the court should not be deprived of the chance to decide in the light of all the circumstances of the case whether one is entitled to privacy or not in those circumstances. The assumption will also reduce unnecessarily the police's exercise of discretion with due respect to the constitutional right to privacy of the person affected.

Unsystematic covert surveillance

4

25. The Monitor queries the need to confine "covert surveillance" to "systematic" ones as proposed in Section 2(1). Covert surveillance should not be exempted simply because it is unsystematically done. The word "systematic" should be dropped in the definition of "covert surveillance" in that section.

Public Officers From Other Jurisdictions

26. There is apparently no provision to prohibit such activities from being conducted by 'public officers' from other jurisdictions, and the Monitor would like a clarification over whether there is any provision which exists to regulate these sorts of activities. In addition, LegCo and the Government should consider whether it is possible to have minor amendments, such as those defining "public officers" to cover public officers from the Mainland as well as foreign public authorities to protect the legitimate right to privacy of all persons in Hong Kong against these outside authorities. All outside law enforcement authorities should not be allowed to conduct any interception of surveillance activities in Hong Kong.
27. Clarification from the Government is also needed on whether there are protection needs to be added to ensure that any material gathered by Hong Kong authorities does not just disappear from the jurisdiction without leaving a record that can be scrutinized locally by the Commissioner on Interception of Communications and Surveillance (the Commissioner).

Notification Procedures and Remedies

28. The Monitor is concerned that in the Bill there are currently no criminal sanctions which "discourages" breaches, only a procedure applying for interception and covert surveillance and a possibility of a victim of a privacy intrusion to be awarded damages by the Commissioner. The Monitor submits that this makes the bill itself ineffective in protecting privacy, since it offers no sufficient deterrence from breach. The Monitor urges the Administration and LegCo Members to introduce amendments to make it an offence

and penalise all internal breaches of the Bill. At the very least, the two criminal offences proposed by the Law Reform Commission should be adopted.

29. In the light of the setting up of the Office of the Commissioner and a power to award damages, the Monitor urges the Administration to explain how a victim would be able to lodge a complaint and claim damages if he is not informed of the wrongful interception of his communication or monitored through covert surveillance. The Monitor would like to know whether it would be possible for example to require the disclosure of such wrongful acts say when there is no concern of undermining any current or prospective law enforcement.
30. There is no provision as to how long materials collected should be kept and how and in what manner they should be disposed of. The Monitor urges the administration to set these out in the legislation and guidelines to ensure that those six principles on privacy of personal information should be adhered to as far as possible with, and used only justifiable exceptions demonstrably necessary in a free society, which are consistent with the ICCPR and other human rights instruments.