立法會

Legislative Council

LC Paper No. LS103/04-05

Comparison of provisions governing authorization to carry out interception of communications or covert surveillance in the Telecommunications Ordinance (Cap. 106), Interception of Communications Ordinance (Cap. 532) and Law Enforcement (Covert Surveillance Procedures) Order

Topic	Section 33 of the Telecommunications Ordinance (TO)	Interception of Communications Ordinance (IOCO)[1]	Law Enforcement (Covert Surveillance Procedures) Order ("the Order")
Authorizing person	The power to authorize interception of messages is vested in the Chief Executive ("CE") or any public officer authorized in that behalf by the CE.	Interception of communications can only be authorized under a court order made by a judge of the High Court upon application by senior officers of certain departments[2] or investigating officers authorized by the Commissioner of the Independent Commission Against Corruption.	The "authorizing officer" in the department concerned. Under the Order an authorizing officer is an officer not below the rank equivalent to that of senior superintendent of police and is designated by the head of the department for that purpose (sections 2, 5(2) and 15).
Grounds for authorizing	The CE may make an order of interception when he considers that the public interest[3] so requires.	Section 4(2) of the IOCO provides that an order shall not be made unless it is necessary for the purpose of preventing or detecting a serious crime or in the interest of the security of Hong Kong. Section 4(3) further provides four	Section 3 provides that the conditions for the grant of an authorization are that - (a) the purpose of the covert surveillance is for preventing or detecting crime, or protecting public safety or security; and

[1] The IOCO, which repeals section 33 of the TO, was enacted in June 1997 but has not yet been brought into operation.

[2] Section 5 of the IOCO provides that the application can only be made by police officers of or above the level of superintendent, senior officers of the Customs and Excise Service, senior officers of the Immigration Department and senior officers of the Correctional Services Department.

[3] The term "public interest" is not defined in the TO, nor is there much case law in Hong Kong explaining what is meant by "public interest". According to some English cases, "public interest" is not to be confused with what interests the public and public opinion (*British Steel Corporation v Granada Television* [1981] 1 All ER 417 at 455, HL, per Lord Wilberforce). While there is no clear definition on "public interest", it was held that whether a particular thing is in the public interest is a question of the times and is a question of fact (*Postmaster General v Pearce* (1923), reported in [1968] 2 QB 463 at 465). It is to be decided in the light of all the circumstances and conditions as they exist at the present notwithstanding that they would probably not have been specifically envisaged by the legislature when an enactment was passed (*Cartwright v Post Office* [1968]2 QB 439).

		matters which the judge is required to determine in deciding whether it is necessary to make an order of interception, namely - (a) whether there are reasonable grounds to believe that an offence is being committed, has been committed or is about to be committed; (b) whether there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) above will be obtained through the interception sought; (c) whether all other methods of investigation have been tried and have failed, or unlikely to succeed; and (d) whether there is good reason to believe that the interception sought will result in a conviction.	(b) the covert surveillance is proportionate to the purpose upon - (i) balancing, in operational terms, the need against the intrusiveness on the subject or other persons who may be affected, and (ii) considering whether the purpose can reasonably be furthered by other less intrusive means.
Types of communications/ information	Messages or class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication may be intercepted. .	Communications in the course of transmission by post or by means of a telecommunication system may be intercepted.	The Order does not specify the type or nature of communications to be obtained by covert surveillance. Section 4 of the Order provides that the Order does not apply to any covert surveillance which is authorized to be carried out by or under any law. Under existing legislation, opening of postal packet could be authorized by the Chief Secretary for Administration under section 13 of the Post Office Ordinance (Cap. 98), and interception of telecommunications could be authorized by the Chief

			Executive under section 33 of the Telecommunications Ordinance (Cap. 106). It is not clear if "law" is intended to have a meaning broader than legislation. The type or nature of communication to be covered by covert surveillance may perhaps be ascertained by reference to the definition of "covert surveillance" in section 2(1) of the Order. There "covert surveillance" is defined to mean "the systematic surveillance of any person for the purposes of a specific law enforcement investigation or operation, if the surveillance - (a) is carried out in circumstances where the person is entitled to a reasonable expectation of privacy; (b) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and (c) is likely to result in the obtaining of any private information about the person".
Scope of order/ authorization	No restriction is imposed on the scope of an order of interception. There are no provisions providing for matters such as the offence or offences in respect of which messages may be intercepted, the method of interception used, etc.	Section 6(1) of the IOCO sets out what are to be specified in the court order, including matters like the offence or offences in respect of which communications may be intercepted, the name and address of the person whose communications are to be intercepted, and the type of communication that may be intercepted and the method of interception used.	There is no provision as to the offences in respect of which covert surveillance may be carried out. As to what are to be specified in the authorization, presumably these would include the items required to be set out in the application. Under section 6 the application shall set out the form of covert surveillance, the information to be obtained, the identity of the subject, particulars of the place, and the proposed duration.

Safeguards for materials obtained	There is no provision on whether the information intercepted pursuant to an order of interception made under section 33 of the TO can be disclosed to other people.	Sections 6, 8 and 9 of the IOCO impose restrictions on the disclosure of the intercepted communications. (a) Section 6(1) provides that a court order authorizing the interception of communications shall specify, among others, the person(s) to whom the intercepted material may be disclosed. (b) Under section 6(2), a judge shall only authorize that the intercepted materials be disclosed to those other law enforcement officers who are involved in the investigation of the offence or offence(s) in respect of which communications may be intercepted. (c) Section 8 imposes a duty on an officer authorized by a court order to intercept a postal communication or telecommunication communication to make arrangements to ensure that the extent to which the intercepted material is disclosed and the number of persons to whom disclosure is made are limited to the minimum that is necessary for the purpose of preventing or detecting a serious crime or in the interest of the security of Hong Kong. Moreover, the relevant authorized officer is required to ensure that	There is no provision on safeguards such as those in section 8 of the IOCO on disclosure of the information obtained, or destruction of the material as soon as its retention is not necessary.

		the intercepted material is destroyed as soon as its retention is not necessary for any of the above purposes. (d) Section 9(4) prohibits a person who is authorized under a court order to intercept a communication to disclose the intercepted material to any other person or persons save for those allowed by the court.	
Duration and renewal of order/authorization	There is no provision providing for the duration of an order of interception.	Section 6(1)(g) of the IOCO provides that the duration for which the interception is authorized must be specified in the court order. Section 6(4) further provides that the authorization under a court order to intercept a communication is valid only for as long as it is necessary to achieve the purpose of interception or, in any event, for a period not exceeding 90 days unless the order is renewed.	Under section 8, an authorization ceases to have effect upon expiration of the period specified by the authorizing officer, which shall not be longer than 3 months. Section 11(4) provides that an authorization may be renewed more than once. Section 12(b) provides that a renewal ceases to have effect upon expiration of the period specified by the authorizing officer, which shall not be longer than 3 months. In urgent cases application for an authorization or renewal may be made orally under section 13. The authorization or renewal granted pursuant to an oral application shall not be longer than 72 hours.
Disposal of material	There is no provision governing the disposal of intercepted material.	Section 7 of the IOCO provides that where a court order authorizing interception has been terminated by the judge or has expired and has not been renewed, all intercepted materials obtained under the court order shall be placed in a packet and sealed by the	There is no provision governing the disposal of material obtained by covert surveillance.

		authorized officer, and that packet shall be kept away from public access. Where no charge is laid against the person named in the court order within 90 days of the termination of a court order, the court may under specified circumstances order the intercepted materials in the sealed packet to be destroyed.	
Remedies for unauthorized interception or disclosure	Nil.	Section 10 of the IOCO provides that the court may on application of an aggrieved person grant remedial relief in respect of unauthorized interception or disclosure when certain criteria are met.	Nil.
Providing information to the Legislative Council (LegCo)	No provision similar to section 11 of the IOCO under the TO[4].	Section 11 of the IOCO confers a statutory power on the LegCo to require the Secretary for Security to provide various types of information relating to interception of communications[5].	No provision similar to section 11 of the IOCO, but the powers and functions of the LegCo referred to in note 4 below is relevant.

Prepared by

Legal Service Division

Legislative Council Secretariat

12 August 2005

[4] Although the LegCo's power to require information relating to interception of messages is not expressly provided in the TO, the LegCo may request the Government to provide such information in exercising its powers and functions under Article 73 of the Basic Law. Under Article 73 of the Basic Law, the powers and functions exercised by the LegCo include the raising of questions on the work of the government and debating any issue concerning public interests.

[5] Such information include the number of interceptions authorized and denied, the nature and location of the facilities from which and the place where the communications have been intercepted, the major offences for which interception has been used as an investigatory method and the number of persons arrested and convicted as a result of interceptions.