Annual Report 2006 to the Chief Executive

by

The Commissioner on
Interception of Communications
and Surveillance

June 2007

截取通訊及監察事務專員辦公室
Office of the Commissioner on Interception of Communications and Surveillance

本處檔號 Our ref.: ICS/1-165/4C　　電話 Tel. No.:

來函檔號 Your. ref:　　傳真 Fax No.:

29 June 2007

The Honourable Donald Tsang GBM
The Chief Executive
Hong Kong Special Administrative Region
People's Republic of China
Government House
Hong Kong

Confidential

Dear Chief Executive,

Annual Report for the Year 2006

I have the pleasure, pursuant to section 49(1) and (6) of the Interception of Communications and Surveillance Ordinance, in submitting to you the annual report for the year 2006, together with its Chinese translation.

Yours sincerely,

(K H Woo)
Commissioner on Interception of
Communications and Surveillance

Encl: Annual Report 2006
and its Chinese translation

香港灣仔皇后大道東 248 號 15 樓 1501 室
Unit 1501 15/F, 248 Queen's Road East, Wanchai, Hong Kong

CONTENTS

ABBREVIATIONS

Unless the context otherwise requires:

added facility, added facilities	facility or facilities additional to those set out in a schedule to an authorization, added pursuant to the 'reasonably expected to use' clause granted in the authorization
C&ED	Customs and Excise Department
Cap	chapter in the Laws of Hong Kong
Code, Code of Practice	the Code of Practice issued by the Secretary for Security under the Ordinance
Commissioner	Commissioner on Interception of Communications and Surveillance
COP forms	specimen forms annexed to the Code of Practice
CSP(s)	communications services provider(s)
ICAC	Independent Commission Against Corruption
ICSO	Interception of Communications and Surveillance Ordinance
Immigration	Immigration Department
interception	interception of communications
internal form, internal forms	one or more of the forms that were produced under the coordination of the Secretary for Security to facilitate LEA officers' tasks under the Ordinance
LEA, LEAs	law enforcement agency, law enforcement agencies

LPP	legal professional privilege
Ordinance	Interception of Communications and Surveillance Ordinance
panel judge	one of the panel judges appointed under section 6 of the Ordinance
PJO	Panel Judges' Office
Police	Hong Kong Police Force
section	section of the Ordinance
statutory activities, statutory activity	interception and surveillance activities called collectively or one of those activities
surveillance	covert surveillance
the report period	the period from 9 August to 31 December 2006
the Team	the dedicated team comprising officers from the LEAs that operates independently of their investigative arms
weekly report forms	the forms designed for the LEAs and panel judges to provide information to the Commissioner

CHAPTER 1

INTRODUCTION AND OBJECTIVE OF THE ORDINANCE

My appointment

1.1 The Interception of Communications and Surveillance Ordinance ('the Ordinance' or 'ICSO') came into force on 9 August 2006 and I was appointed as the Commissioner on Interception of Communications and Surveillance ('Commissioner') by the Chief Executive on the same date to take effect on 17 August 2006. The appointment was made pursuant to section 39 of the Ordinance and was for a period of three years.

Objective of the Ordinance

1.2 The Ordinance prohibits public officers from directly or indirectly carrying out any interception of communications ('interception') and any covert surveillance ('surveillance') [sections 4(1) and 5(1)] (collectively called 'statutory activities' in this report) unless it is done pursuant to a prescribed authorization [sections 4(2) and 5(2)].

1.3 The conditions for the issue, renewal or continuance of a prescribed authorization are set out in section 3. The conditions are threefold: first, circumscribing the purposes sought to be furthered by carrying out a statutory activity, which are for preventing or detecting serious crime or for protecting public security; second, requiring that there be reasonable suspicion in relation to the serious crime or the threat to public security involved; and third, stipulating the requirements of necessity and proportionality having to be satisfied. It is only where the

intrusion by the statutory activity into privacy of the person is necessary and reasonably proportional to the furtherance of the purposes of fighting serious crime or protecting public security that it should be permitted, and even then the possibility of employing other less intrusive means should always be considered.

1.4 The objective of the Ordinance is thus made abundantly clear. It is for the protection of the rights of persons in Hong Kong (see Article 41 of the Basic Law) in various facets of privacy that are protected by Article 29 of the Basic Law (prohibition against arbitrary or unlawful intrusion into a home or other premises), Article 30 of the Basic Law (prohibition against infringement of privacy of communications) and Article 17 of the International Covenant on Civil and Political Rights (incorporated in Article 14 of the Hong Kong Bill of Rights Ordinance, Cap 383) (prohibition against interference with privacy, family, home and correspondence and against attacks on honour and reputation), as enshrined by Article 39 of the Basic Law. It is only where the conditions and requirements of the Ordinance have been satisfied that a prescribed authorization may be granted to public officers to carry out and continue with a statutory activity.

Misunderstood name

1.5 However, right upon my assumption of office as Commissioner, I felt that some members of the media and the public seemed to consider that the panel judges (referred to in the following paragraph) and I were appointed to assist the law enforcement agencies ('LEAs') in their conducting statutory activities in disregard of the privacy of persons in Hong Kong. This view, which is contrary to the clear

objective of the Ordinance, might have been caused by the title of the Ordinance and that of the Commissioner. Had the Ordinance been named, for example, as the Protection against Unlawful Interception of Communications or Surveillance Ordinance and my post been called the Commissioner on Protection against Unlawful Interception of Communications or Surveillance, I would have thought that that would have eliminated the misunderstanding and generated a better appreciation of the objective of the Ordinance and the purposes of my appointment.

General scheme

1.6 The general scheme of the Ordinance may be briefly described as follows. Surveillance is divided into two types: the more intrusive surveillance is called Type 1 and the less Type 2 [see their respective definitions in section 2(1) and paragraphs 6.1, 6.4 and 7.1 below]. A panel of judges ('panel judges') is to be appointed [section 6] for dealing with applications made by the LEAs for interception and Type 1 surveillance. Each application is to be determined by a panel judge. In handling an application, the panel judge concerned must examine the application presented before him and may grant a prescribed authorization only where the requirements of the Ordinance are satisfied. For Type 2 surveillance, the applications by the LEAs are to be dealt with by an authorizing officer of not below the rank of senior superintendent of police or equivalent [section 7], who may grant a prescribed authorization upon the same requirements being met.

1.7 A Commissioner is to be appointed with various functions [Part 4 of the Ordinance], the main aim being to ensure full compliance with the requirements of the Ordinance by the LEAs under his power of

oversight and review. He has a further function, which is to examine and determine applications from members of the public who claim that any of the LEAs have carried out a statutory activity against them and to order compensation to be paid by the Government to applicants in whose favour a case of conduct of any such activity without a proper prescribed authorization has been found.

This report

1.8 The Commissioner shall report to the Chief Executive at regular intervals [section 49(1)]. The first report is to cover the period from the commencement of the Ordinance to 31 December 2006 ('the report period' or 'this report period') whilst later reports are to cover subsequent yearly periods [section 49(6)]; and each report is to be submitted within six months after the end of the period covered [section 49(3)].

1.9 This is my first report.

Limit of transparency

1.10 In performing his functions under the Ordinance, the Commissioner shall take heed not to divulge any information the disclosure of which may prejudice the prevention or detection of crime or the protection of public security. For instance, I am not allowed to disclose to an unsuccessful applicant for examination the reason why I have reached the determination of finding not in favour of his case [section 46(4)(a) and section 48(4)(a)] or even indicate whether any statutory activity complained of has taken place [section 46(4)(c)]. Even if I were to find a case in favour of the applicant, I should only give him a notice leading to my assessing compensation to be awarded to him if I consider that my so

doing would not be prejudicial to the prevention or detection of crime or the protection of public security [section 44(6)].

1.11 Thus, it is incumbent upon me to consider very carefully what should be disclosed in this report as well as to the public so as to ensure that no prejudice as envisaged by the Ordinance will be caused. This is the reason why some matters in this report may not be described in as much detail as one would like.

1.12 Indeed, there is a further safeguard provided by the Ordinance regarding the contents of my report, which is that the Chief Executive may exclude any matter in the report the publication of which he considers would result in the prejudice being caused [section 49(5)].

CHAPTER 2

FUNCTIONS AND AREAS NOT COVERED BY THE ORDINANCE

My functions

2.1 My functions as Commissioner are set out in Part 4 of the Ordinance under six Divisions. Section 40 summarizes my main functions as follows:

(a) to oversee the compliance by the LEAs, referred to in paragraph 2.7 below, and their officers with the statutory requirements (Division 1);

(b) to conduct reviews that I consider necessary with regard to such compliance (Division 2);

(c) to carry out examinations upon receiving written applications from persons of their suspicion of having been subject to interception or surveillance by an LEA, and upon finding a statutory activity without the authority of a prescribed authorization having been conducted against an applicant, to determine the compensation and order payment of it to him (Division 3);

(d) to notify the person against whom I have discovered that any interception or surveillance having been carried out by an LEA without the authority of a prescribed authorization, and to determine the compensation and order payment of it to him upon his application for examination (Division 4);

(e) to submit reports to the Chief Executive, to make recommendations whenever necessary to the Secretary for Security regarding the Code of Practice issued by him to the LEAs for practical guidance in respect of matters under the Ordinance, and to make recommendations to heads of the LEAs for a change of any arrangements made by them to better carry out the objects of the Ordinance (Division 5); and

(f) to perform any other or further functions as are imposed by the Ordinance or any other enactment and as are prescribed by any regulation made under the Ordinance by the Chief Executive (Division 6).

2.2 Since as the Commissioner, I am only concerned with various facets of the working of the Ordinance as aforesaid, it is necessary to set out what the Ordinance does not encompass so that the sphere of my functions will be better understood.

Matters beyond the Ordinance

2.3 The Ordinance prohibits interception and surveillance being carried out by any public officer except pursuant to a prescribed authorization [sections 4 and 5]. There is no express provision prohibiting such activities by persons other than public officers.

2.4 'Interception' is defined in section 2(1) as meaning the inspection of some or all of the contents of any communication, in the course of its transmission by a postal service or by a telecommunications system, by a person other than its sender or intended recipient. This definition is very wide.

2.5 On the other hand, 'covert surveillance' is defined in section 2(1) as follows:

> '(a) [It] means any surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation, if the surveillance –
>
> (i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;
>
> (ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and
>
> (iii) is likely to result in the obtaining of any private information about the person; but
>
> (b) does not include –
>
> (i) any spontaneous reaction to unforeseen events or circumstances; and
>
> (ii) any such surveillance that constitutes interception under this Ordinance[.]'

2.6 Thus, as a matter of general application and in the usual circumstances that can be envisaged, where the surveillance is not carried out with the use of any surveillance device, or where the person subject to surveillance is not entitled to a reasonable expectation of privacy, or where the surveillance is a spontaneous reaction to unforeseen events or circumstances, then it is not a form of surveillance that is covered by the Ordinance and therefore is not within my remit as Commissioner. The exception in paragraph (b)(ii) of the definition, ie where the surveillance constitutes an interception under the Ordinance, does not affect the protection of privacy offered by the Ordinance because this form of surveillance is covered by and subjected to the statutory requirements relating to interceptions.

2.7 My remit as Commissioner only concerns the LEAs (and their officers) as specified in Schedule 1 to the Ordinance, namely, Customs and

Excise Department ('C&ED'), Hong Kong Police Force ('Police') and Independent Commission Against Corruption ('ICAC') in relation to interception, and C&ED, Police, Immigration Department ('Immigration') and ICAC in relation to surveillance. I am not concerned with persons other than those public officers who may engage in interception and surveillance, nor am I concerned with any forms of surveillance not within the definition of that term under the Ordinance.

2.8 An example can be given to demonstrate the limit of my functions. If a person makes an application for examination to me under Division 3 of Part 4 of the Ordinance, and my finding is that the interception or surveillance suspected by the applicant is not within the definition of those terms in the Ordinance or alternatively that the suspected activity has been carried out other than by an LEA, my task is to give a notice to the applicant that I have not found the case in his or her favour.

Possible remedies

2.9 In such a situation, any remedy that the applicant may seek depends on the circumstances of his case. A good summary of the various remedies available under existing laws can be found in Chapter 2 of The Law Reform Commission's Report on Civil Liability for Invasion of Privacy published in December 2004.

CHAPTER 3

LEGAL PROFESSIONAL PRIVILEGE AND JOURNALISTIC MATERIAL

Introduction

3.1 The Ordinance makes specific reference to legal professional privilege ('LPP') and journalistic material for particular caution when statutory activities are to be authorized and carried out.

Protection

3.2 The right of Hong Kong residents to confidential legal advice is protected by Article 35 of the Basic Law. This is to recognise the well-established common law right to LPP. The right is not only a rule of the law of evidence prohibiting the disclosure in court proceedings of information subject to the privilege without the consent of the person enjoying the privilege, but is also fundamental to the protection of the individual in his access to the courts and to the fulfilment of the system of administration of justice.

3.3 On the other hand, the freedom of the press, the principal manifestation of the freedom of expression, and the various forms of freedom of expression are enshrined in Article 27 of the Basic Law.

3.4 Section 2(3) of the Ordinance elevates any Type 2 surveillance as Type 1 surveillance if it is likely that any information which may be subject to LPP will be obtained by carrying out the surveillance. Type 2 surveillance is one that can be authorized internally by an authorizing officer within the LEA itself, whereas Type 1 surveillance must be

authorized by a panel judge. Moreover, section 31 provides that save for exceptional circumstances, no interception or surveillance should be authorized by reference to the premises of a lawyer, including his office and residence, or to his communications. In the applications for interception and surveillance, attention of the relevant authorizing authority (panel judge or authorizing officer or head of department) is required to be drawn as to the likelihood of obtaining any LPP information (see Part 1 paragraph (b)(ix), Part 2 paragraph (b)(x) and Part 3 paragraph (b)(x) of Schedule 3 to the Ordinance).

3.5 Although journalistic material is not given as much prominence in the body of the Ordinance as LPP save in the various provisions of Schedule 3 to the Ordinance referred to above, attention of the relevant authorizing authority is similarly required to be drawn to the likelihood of journalistic material being obtained in an application for interception or surveillance.

3.6 The aim of these statutory provisions is to ensure that where it is likely that LPP information or journalistic material will be obtained, the application for authorization must be scrutinized most carefully, offering better protection of the right to confidential legal advice and the freedom of the media.

The LEAs' practice

3.7 In accordance with the aim and spirit of the Ordinance, I have paid heed to LPP information and journalistic material when performing my reviewing functions in the context both of the authorization process and the investigation product in order to prevent any abuse or dilution of these fundamental rights.

3.8 In the sample form of affidavit/affirmation (hereinafter called 'affidavit') in support of the application to a panel judge for prescribed authorization, it can be found that the LEAs' attention is directed to the subjects of LPP information and journalistic material. Where LPP information or journalistic material might possibly be involved or obtained, the LEA's affidavit would state the possibility.

3.9 From the review that I have conducted, I found that where there was a likelihood of LPP information being obtained, the panel judge adopted a cautious approach in determining the application, and even when granting the authorization sought, he would impose stringent conditions in the authorization such as the LEA would have to report to him as a material change of circumstances if LPP information was obtained, thus retaining the power to review the situation if and when the need should arise.

3.10 The LEAs have to assess whether LPP information or journalistic material may be obtained and to disclose their assessment to the panel judge. From my checking of the LEAs' files, I have found that they do pay heed to these two matters, that they disclose their assessments to the panel judges and that their assessments are reasonable under the circumstances.

3.11 In all the cases reported to me by the LEAs during the report period, there was not a single case where journalistic material was ever obtained. Nor was there a case where LPP information had in fact been obtained.

CHAPTER 4

PROCEDURE OF OVERSIGHT AND REVIEW OF LEAS' COMPLIANCE

Procedure of oversight

4.1 Shortly after I took office, I started with requiring weekly reports from the panel judges and the LEAs on the applications for statutory activities, successful or otherwise, by way of requiring them to fill in forms designed with the assistance of my Secretariat for the purpose ('weekly report forms'). The first report was to cover the period from the commencement of the Ordinance on 9 August till 25 August 2006. The literally weekly reporting started from the period from 26 August to 1 September 2006 and subsequent reports were to cover each calendar week thereafter. Up to the end of this report period, the Panel Judges' Office ('PJO') and the LEAs had each furnished me with 19 reports. The aim was to establish a constant checking system to ensure that any discrepancy between the returns from the PJO and the LEAs would be revealed timely. A second aim was to discover any impropriety or deficiency as soon as practicable so as to be able to nip it in the bud.

4.2 In the second weekly returns, it was disclosed that an LEA had granted two Type 2 surveillance authorizations, which were said to be premises-based, with the use of a listening device. According to the definition of Type 2 surveillance under section 2(1) of the Ordinance, where a listening device is used, the minimum requirement is that the person using the device should be the intended or expected recipient to hear the words spoken by the targeted person, or the person using the device

listens to, monitors or records the words or activity with the consent, express or implied, of the intended or expected recipient. It was most unlikely that such Type 2 surveillance would be premises-based (directed at a fixed place) instead of subject-based (ie, directed at a targeted person).

4.3 Thus, I was wondering if the premises-based operations were in fact squarely within Type 2, so that the authorization could properly have been granted by an authorizing officer of the LEA, instead of being sought from a panel judge. I immediately had the LEA contacted so that I could conduct an inspection of the files relating to the two applications. A visit to the LEA was soon arranged for me to check the two files.

4.4 The inspection was made by me in the presence of an assistant head of the LEA and two other officers. I was informed that the surveillance operations carried out pursuant to the two Type 2 authorizations had already been discontinued and a report had been made to the authorizing officer who had revoked them. I checked the two related files. The first one involved the use of a listening device installed on a person (Person A) who was in possession of a prohibited article and who had provided information that someone (unknown and unidentified) would be contacting Person A to receive the prohibited article while Person A stayed inside known premises. The second case involved a similar operation with a different person (Person B) inside another known premises. However, there was an added listening device installed on the mobile phone of Person B so that the device would record the conversation Person B might have with anyone contacting Person B over that mobile phone. The person in both cases would turn on the listening and recording device whenever the situation required, and intrusion into the privacy of anyone who was not the recipient of the prohibited article would unlikely be

involved. I was satisfied that both operations were within the ambit of Type 2 surveillance, in which the persons using the listening devices were the intended or expected recipient to hear the words spoken by the targeted persons.

4.5 Notwithstanding, I took the opportunity to advise the officers of the LEA that their weekly report on the second case should not have simply stated that the surveillance was premises-based; they should have added that it was also object-based, because they applied the additional listening and recording device to the mobile phone held by Person B. The officers undertook to amend the related weekly report in order to remedy the slight deficiency.

4.6 This checking of the records of the applications had eliminated my fear that the LEA had not complied with the requirements of the Ordinance. My concern was caused by the lack of imagination on my part as to how premises-based listening surveillance could have been carried out as Type 2 surveillance. The review of the files had also enabled me to advise the LEA how the weekly report forms should be properly filled. It also had the effect, as intended, of demonstrating that I, as the Commissioner, am vigilant in performing my duties of ensuring full compliance with the statutory requirements and that everything the LEAs do will be under my watchful eye.

4.7 The above description of the first encounter with an LEA is to demonstrate the general nature of my visits to the premises of the LEAs and the checking of the relevant files they kept for the purpose of clarification and verification, wherever necessary. I also conducted random checks of files relating to the successful and unsuccessful applications for a

statutory activity, even where there was no necessity to seek clarification. During such visits, I also took the opportunity to review the relevant procedures and arrangements and advised improvements to be made if and when so required.

Other steps taken

4.8 Apart from counter-checking the weekly returns from LEAs against those from the PJO, and conducting periodical checks of the relevant files and documents at the LEAs' offices, I have also adopted measures for further checking respectively the interceptions and surveillance conducted by the LEAs.

4.9 Wherever necessary, a counter-check has been conducted with non-LEA parties such as communications services providers ('CSPs') who have played a part in some of the interception process but are independent from the LEAs. The interceptions by an LEA are made through a dedicated team ('the Team') that, whilst being part of the LEAs, operates independently of their investigative arms. With telecommunications interception effected through the CSPs, for example, I required the CSPs to verify the facilities intercepted against the prescribed authorizations produced by the Team for checking and to notify me if any interception was done without authorization. I also required the CSPs to furnish me with a four-weekly return to ensure that the number of facilities intercepted tally with those as reported by the LEAs. I consider it would not be prudent, for security reasons, to divulge any further details of the procedures of how interception requests were made to the CSPs, how the requested interceptions were effected and how my checking exercises were conducted.

4.10 For surveillance, the weekly returns from the LEAs have been counter-checked against the PJO's returns. In case of any discrepancies, clarifications and explanations were sought from the LEA concerned and the PJO. The periodical physical checks of the LEA files and documents and the requirement of explanations were also carried out to clarify any doubts or suspicions that I harboured. In addition, I required each of the LEAs that are entitled to apply for authorization for surveillance to prepare inventories of surveillance devices stored and registers of withdrawal and return of such devices so as to enable me to check if any such device had been drawn out and made use of by officers for authorized surveillance purposes or otherwise. More details on this matter can be found in paragraphs 6.26 to 6.30 of Chapter 6.

Review of compliance

4.11 On the whole, the LEAs were extremely cooperative and all my queries and doubts have been clarified. I have not detected any intentional or deliberate contravention of the requirements of the Ordinance by any LEA or its officers.

4.12 The panel judges on the whole have applied the requirements of the Ordinance in a stringent manner in their consideration of the applications made by the LEAs. For instance, at the initial stage a high number of an LEA's applications for interception and surveillance were rejected, mainly for the reason that the panel judges considered that insufficient material was provided in the applications to justify the necessity of operating the statutory activities for the period applied for, especially where that period was the maximum period that can be authorized under the Ordinance.

4.13 There was an occasion that the affidavit in support of the application stated that 'there has been no issue of any prescribed authorization in which (the subject) has been subject to interception' within the preceding two years but at the oral hearing before a panel judge the applicant revealed that in fact interception activities had been carried out against the targeted person pursuant to an authorization under the former regime before the ICSO came into existence. The LEA concerned considered that the term 'prescribed authorization' meant an authorization under the Ordinance because it was the term used and interpreted as such in the Ordinance, and that any prior authorization under the former regime was not a prescribed authorization. Thus what was stated in the affidavit was considered by the LEA to be factually correct. The panel judge who dealt with the application, however, considered that the statement in question was 'woefully misleading' since the Ordinance only came into existence on 9 August 2006. He refused the application, taking the view that it was incumbent upon the applicant to provide evidence that 'paints a full and complete picture to the relevant authority', and that the applicant's statement in the affidavit did not do so and instead it misled. It was the common opinion held by all the three panel judges that since applications made by the LEAs under the Ordinance are necessarily *ex parte* applications, the normal rule applicable to *ex parte* applications, ie, that it is the duty of the applicant to make full and frank disclosure of all facts material to the application, should apply to the LEAs. Not disclosing the authorization under the former regime relating to the targeted person fell foul of the rule. Paragraphs 9.14 to 9.19 of Chapter 9 are also relevant. I understand that after this case, the LEAs have paid extra attention to the accuracy of information that they present to support their applications. They understand that to enable the relevant authority to make a balanced

decision, apart from information required to be provided under the Ordinance, all information known to the applicant to be relevant to the determination of an application should be provided.

4.14 The panel judges were extremely cautious in considering applications by LEAs if it was likely that information which might be subject to LPP might be obtained. For example, where the targeted person had been arrested, the panel judge would consider carefully whether any further conduct of a statutory activity would likely contravene LPP. In some cases, authorization was refused on this ground.

4.15 There was also a case where no useful information had been obtained by the LEA after the authorized interception had been granted for about three months, the panel judge refused a third renewal of the authorization.

4.16 The panel judges' reasons for refusal of LEAs' applications, as revealed by my checking, have led me to conclude that the panel judges have applied very stringent tests in their consideration of the applications and that they have conscientiously applied the Ordinance's requirement that an authorization should only be granted upon the proportionality test being fully satisfied. In my view, the panel judges might on occasions be said to have acted over-cautiously.

4.17 Thus, I am quite sure that authorizations granted by the panel judges were all made properly. The panel judges have helped to ensure that only where there is a need for the purposes of preventing or detecting serious crime or of protecting public security and that the statutory activity is proportional that they will grant an authorization for such activity to be carried out.

4.18 Moreover, there were cases which demonstrate that insofar as the purpose sought to be achieved could not be achieved by an authorized statutory activity, the LEA concerned terminated such activity. This is not limited to the usual circumstances under section 57 – discontinuance of the activity, or under section 58 – decision of the authorizing authority to revoke an authorization after receipt of a report on arrest of the targeted person. For example, the LEA which had been duly authorized to intercept a telecommunications facility (such as a telephone line) might discontinue the operation where the interception so far carried out for a short period had not produced any discernible result to help investigation. However, there were cases where the discontinuance was reported to the PJO for the reason that useful information had been elicited through the interception, but the LEA discontinued the interception instead of trying to obtain more information. There were also cases where the LEA reported the reason for discontinuance as being the subject having withdrawn from the criminal plot. These cases reflect that the LEAs had complied with the requirements of the Ordinance in not simply adopting a passive attitude by leaving matters continue until the expiration of the authorized period for the statutory activity. They had apparently heeded and borne in mind that intrusion into privacy, even of the suspected criminal, should not go unchecked, and whenever circumstances did not require the intrusion being continued, they would vigilantly take the initiative to discontinue the activity.

4.19 There was no application for emergency authorization for any statutory activity in the report period. There were possibly two reasons. First, there was no case falling within circumstances that required an emergency authorization. Second, the LEAs might have paid careful

regard to the statutory requirements and would not lightly embark upon an application for emergency authorization unless the conditions to be complied with were met. Regardless of whether such caution stemmed from the LEAs' respect for the law or from the apprehension of the panel judges' strict control, it would, if existed, reinforce the protection of privacy.

4.20 The stringentness of the panel judges in their consideration of the applications and the LEAs' heed to the requirements of the Ordinance have made me doubly sure that any statutory activity carried out by the LEAs as authorized by the panel judges was proper, and any interception or surveillance so authorized was engaged only when required under the circumstances as prescribed by the Ordinance, thus ensuring that intrusion into the privacy of persons in Hong Kong was kept to the minimum.

CHAPTER 5

INTERCEPTION

Definition

5.1 Under the Ordinance, the definition given to an 'intercepting act', as a necessary ingredient of 'interception', in relation to any communication, is the carrying out of inspection of some or all of the contents of the communication by a person other than its sender or intended recipient. The communication under inspection is in the course of its transmission either by a postal service or by a telecommunications system.

A brief overview of the legislation on interception

5.2 The primary objective of the legislation is to protect the privacy of individuals who use postal service or telecommunications systems in Hong Kong for communication purposes. The Ordinance also specifies the legal framework for authorized interception to be carried out.

5.3 Under section 4 of the Ordinance, no public officer shall directly or indirectly carry out any interception. This prohibition 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 radiocommunications 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 the 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).

5.4 As specified in section 3(1) of the Ordinance, the purpose sought to be furthered by carrying out interception pursuant to a prescribed authorization is that of 'preventing or detecting serious crime'[Note 1] or 'protecting public security'.

Prescribed authorizations

5.5 Under section 29(1) of the Ordinance, a prescribed authorization for interception may –

(a) in the case of a postal interception, authorize one or both of the following –

(i) the interception of communications made to or from any premises or address specified in the prescribed authorization;

(ii) the interception of communications made to or by any person specified in the prescribed authorization; or

(b) in the case of a telecommunications interception, authorize one or both of the following –

(i) the interception of communications made to or from any

Note 1 'Serious crime' in relation to a prescribed authorization for interception means any offence punishable by a maximum penalty that is or includes a term of imprisonment of not less than seven years [section 2(1) of ICSO].

telecommunications service specified in the prescribed authorization;

(ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization is using, or is reasonably expected to use.

5.6 What requires specific mention is the last category where the authorization allows interception of a telecommunications facility (such as a telephone line) that the targeted person is 'reasonably expected to use', although when the authorization is granted, the identifying details of the facility (such as the telephone number) are not yet known. This kind of authorization gives the LEA concerned the power to include a facility in the authorization identified only after the grant of the authorization and conduct interception of it without the necessity of going back to the panel judge to obtain specific authorization regarding it. This matter will be further discussed in Chapter 11 and Chapter 13. I have paid particular attention to this type of authorization and am glad to report that I have not found a case where the panel judge had granted any such authorization inappropriately or a case where the LEA concerned had subsequently added a facility without justification.

5.7 Schedule 1 to the Ordinance specifies the LEAs that may carry out interception under a prescribed authorization. They are the C&ED, the Police and the ICAC. Thus, the law is clear that out of the four law enforcement departments specified under the Ordinance, Immigration alone has not been conferred any power to carry out interception. The reference to LEAs in this chapter, therefore, must be read to exclude that Department.

Judges' authorizations

5.8 An officer of an LEA may apply to a panel judge for the issue of a judge's authorization or renewal for any interception to be carried out. The application is to be made in writing and supported by an affidavit of the applicant. The Ordinance does not allow interception to be authorized by an 'executive authorization' that applies only to Type 2 surveillance. The maximum duration authorized for an interception allowed for by the Ordinance is in any case not to be longer than the period of three months [section 10(b)]. The same maximum duration is also set for renewal of such an authorization [section 13(b)].

Emergency authorizations

5.9 An officer of an LEA may apply to the head of the department for the issue of an emergency authorization for any interception, if he considers that there is immediate need for the interception to be carried out by reason of an imminent risk of death or serious bodily harm, substantial damage to property, serious threat to public security or loss of vital evidence, and that it is not reasonably practicable to apply for the issue of a judge's authorization, having regard to all the circumstances of the case [section 20(1)]. An emergency authorization shall not last for more than 48 hours and may not be renewed [section 22(1)(b) and (2)]. The officer should also apply to a panel judge for confirmation of the emergency authorization within 48 hours, beginning with the time when the emergency authorization is issued [section 23(1)].

5.10 During the report period, no application for emergency authorization for interception was ever made by any of the LEAs.

Oral applications

5.11 An application for the issue or renewal of a prescribed authorization may be made orally if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provisions under the Ordinance. This practicability condition must be satisfied for the grant of authorization upon an oral application [section 25(2)]. An oral application and the authorization granted as a result of the application are regarded as having the same effect as a written application/authorization. The officer concerned should also apply for confirmation of the prescribed authorization within 48 hours beginning with the time when the authorization is granted. See sections 25 to 27 of the Ordinance.

5.12 During the report period, no oral application for interception was ever made by any of the LEAs.

Written applications

5.13 A total of 485 written applications for interception were made by the LEAs during the report period. The number of judges' authorizations issued was 449, of which 301 were made pursuant to fresh applications and 148 were consequent upon renewal applications[Note 2]. Altogether, 30 fresh applications and five renewal applications for interception had been refused by the panel judges. One renewal application was granted but no authorization was in fact issued due to the fact that the

Note 2 The number of applications granted does not necessarily equal the number of investigation cases. A particular investigation case could involve more than one application for interception / surveillance.

subject of the interception was arrested after the submission of the application.

Offences

5.14 A list of the major categories of offences for the investigation of which prescribed authorizations for interception had been issued or renewed during the report period is shown in Table 2(a) in Chapter 12.

Duration of authorizations

5.15 For the majority (over 83%) of the cases (fresh authorizations as well as renewals), the duration of the prescribed authorizations granted by the panel judges lasted for a period of one month or less, a duration that was relatively short as compared to the maximum of three months allowed by the Ordinance [sections 10 and 13]. Only one authorization was granted for a period of three months. Apparently, the panel judges were acting cautiously and applying a rather stringent control over the use of interception activity by the LEAs. Overall, the average duration for interception authorized during the report period was one month.

Revocation of authorizations

5.16 Under section 57(1), an officer of an LEA, who conducts any regular review pursuant to the arrangements made under section 56 by his head of department, should cause an interception (and also surveillance) to be discontinued if he is of opinion that the ground for discontinuance of the prescribed authorization exists. A similar obligation also attaches to the officer who is for the time being in charge of the interception after he becomes aware that such a ground exists [section 57(2)]. The officer concerned shall then report the discontinuance and the ground for

discontinuance to the relevant authority who shall revoke the prescribed authorization concerned [section 57(3) and (4)].

5.17 The number of authorizations for interception revoked 'fully' pursuant to section 57 during the report period was 156. In addition, another 26 cases involved the cessation of interception in respect of some but not all of the communications facilities approved under a prescribed authorization, so that interception of the other facilities remained in force. Such 'partial' revocation is also dealt with in paragraphs 11.4 to 11.10 of Chapter 11 and paragraphs 13.5 to 13.7 of Chapter 13. The normal grounds for discontinuance were mainly situations where the subjects were arrested, or that continuing with the interception was not useful because the communications facility was found not used or seldom used by the targeted subject.

5.18 Revocation of authorizations is also provided for in section 58 of the Ordinance. Where the relevant authority receives a report from an LEA that the subject of an interception has been arrested, with an assessment of the effect of the arrest on the likelihood that any information which may be subject to LPP will be obtained by continuing the interception, he shall revoke the prescribed authorization if he considers that the conditions for the continuance of the prescribed authorization under the Ordinance are not met. The number of revocations under section 58 during the report period was eight.

5.19 It will be noted that whereas section 57 covers the situation where discontinuance has already taken place and the only thing to be done by the relevant authority is to revoke the authorization (section 57(4): 'shall revoke') without any necessity to exercise discretion, section 58 imposes

two requirements, namely, first the assessment by the reporting officer of the effect of the arrest on the likelihood that LPP information may be obtained by continuing with the interception authorized and second, the consideration by the relevant authority after receiving the report of arrest whether 'the conditions for the continuance of the prescribed authorization under section 3 are not met' and he 'shall revoke the prescribed authorization' if he so considers [section 58(2)].

5.20 It was at first not clear if section 57 could be applied if there was an arrest of the subject targeted by the activity authorized by a prescribed authorization. After discussions amongst the Security Bureau, the LEAs, the panel judges and the Commissioner, it was agreed that only where the reporting officer of the LEA requires the relevant authority to make consideration and exercise discretion under section 58(2) that he should make a report under section 58; in all other cases, where a ground for discontinuance arises, a report should invariably be made under section 57 that would result in the revocation of the prescribed authorization. The discrepant practices that had originally been used were eliminated and a unified practice was thus adopted.

Legal professional privilege

5.21 During the report period, there was no case in which information subject to LPP had been obtained in consequence of interception carried out pursuant to a prescribed authorization.

5.22 It was however noted that a small proportion of applications for interception were assessed to have the likelihood of LPP information being obtained. Some of them were refused by the panel judges. I have checked all the files regarding these cases during my inspection visits at the

LEAs' premises. It appears to me that the panel judges had considered the cases carefully and had reasonably assessed the likelihood of LPP information being obtained, amongst other factors concerned in respect of the case, in reaching the decision that the interception applied for should or should not be authorized.

Effectiveness of interception

5.23 Among the LEAs, there is a common view that interception is and continues to be an effective and valuable investigation tool. Information gathered from interception can lead to a fruitful and successful conclusion of an investigation. During the report period, a total of 59 persons, who were subjects of authorized interception operations, were arrested as a result of or further to interceptions carried out pursuant to prescribed authorizations. In addition to the arrests of subjects in the interceptions, a total of 71 non-subjects were arrested as a result of or further to interceptions carried out pursuant to prescribed authorizations. The relevant arrest figures are shown in Table 3(a) in Chapter 12. The benefit of interception as an investigation tool can therefore be appreciated.

Cases of irregularities

5.24 During the report period, there were two reports of irregularities concerning three cases of interception operations. Details of the cases can be found in Chapter 10.

5.25 In addition, one LEA officer had committed a minor typographical error in the spelling of the name of the targeted person in the granted prescribed authorization while that person's identity card number and other particulars were correctly stated. The mistake was not

discovered until an application for renewal was made to the panel judge. He directed that the error be corrected. The case was rightly not treated as an irregularity since no one other than the targeted person was affected by the prescribed authorization and that the error was corrected upon discovery. It was merely caused by a careless mistake and did not have any impact on any other person. The LEA concerned was, however, frank and prompt in its weekly report to me (see below) to draw my attention to this case.

Checking of cases

5.26 The LEAs and the PJO are required to submit weekly reports to the Commissioner's Office on every application for interception approved or refused during the week. Information such as the identifying details of the communications facility (eg telephone lines added pursuant to the 'reasonably expected to use' clause referred to in paragraph 5.6 above), duration of authorization, offences involved, together with other relevant details submitted by a party is verified against information provided by another party to check if there was any irregularity involved. Towards the end of the report period, information on interceptions was also required from the Team of the LEAs (referred to in paragraph 4.9 of Chapter 4) and from CSPs, whenever necessary, to provide another source for counter-checking, clarification and verification purposes.

5.27 Visits to the LEAs for checking purposes were also carried out on a regular basis periodically. The LEAs were requested to explain their operational procedures, to provide the original of the applications and other relevant documents for checking and to answer my queries on any doubtful cases. Whenever circumstances require, applicants of prescribed

authorizations and other officers responsible for matters relating to the interceptions were interviewed. In the course of checking, where I found any areas requiring improvement, I had advised the LEAs and made recommendations to them for implementing appropriate measures. A total of 138 interception-related cases were checked. Apart from those cases involving irregularities referred to in paragraph 5.24 above and those in paragraph 13.38 of Chapter 13, no other irregularity had been observed during the checking. I found no evidence whatsoever that any of the LEAs had wilfully not complied with the requirements of the Ordinance.

CHAPTER 6

TYPE 1 SURVEILLANCE

Covert surveillance

6.1 Under the Ordinance, officers of the LEAs are required to obtain a prescribed authorization for carrying out any 'covert surveillance' operation. A prescribed authorization can be issued either by a panel judge ('judge's authorization') or a designated authorizing officer[Note 3] within the individual LEA ('executive authorization'). Section 2(1) of the Ordinance defines 'covert surveillance' as:

> 'any surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation, if the surveillance –
>
> (i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;
>
> (ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and
>
> (iii) is likely to result in the obtaining of any private information about the person; …'

According to the above definition, other kinds of surveillance conducted in circumstances where a person is not entitled to a reasonable expectation of privacy is not considered as 'covert surveillance'. Prescribed authorization is therefore not required for such kind of 'non-covert surveillance'. An example of 'non-covert surveillance' is surveillance upon a person's activities in a public place where such activities can be visible to other passers-by without the aid of a sense-enhancing device (surveillance device).

Note 3 Section 7 of ICSO refers an authorizing officer as an officer designated by the head of department not below a rank equivalent to that of senior superintendent of police.

6.2 Equal to interception, the Ordinance confines the purposes sought for surveillance operation by its section 3(1) to 'preventing or detecting serious crime'[Note 4] or 'protecting public security'.

6.3 For the report period, all applications for surveillance, including those granted and those refused, were sought for the statutory purposes.

Type 1 surveillance versus Type 2 surveillance

6.4 Section 2(1) of the Ordinance only gives a very simple definition of Type 1 surveillance as '*any covert surveillance other than Type 2 surveillance*'. Basically these two types of surveillance can be distinguished by their different degrees of intrusiveness into a person's privacy: Type 1 surveillance is more intrusive than Type 2 surveillance. Type 2 surveillance is defined in section 2(1) of the Ordinance as meaning any surveillance that –

> '(a) is carried out with the use of a listening device or an optical surveillance device by any person for the purpose of listening to, monitoring or recording words spoken or activity carried out by any other person, if the person using the device –
>
> (i) is a person by whom the other person intends, or should reasonably expect, the words or activity to be heard or seen; or
>
> (ii) listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i); or
>
> (b) is carried out with the use of an optical surveillance device or a tracking device, if the use of the device does not involve –
>
> (i) entry onto any premises without permission; or

Note 4 'Serious crime' in relation to prescribed authorization for surveillance means any offence punishable by a maximum penalty that is or includes a term of imprisonment of not less than three years or a fine of not less than $1,000,000 [section 2(1) of ICSO].

(ii) interference with the interior of any conveyance or object, or electronic interference with the device, without permission.'

6.5 Section 2(3) of the Ordinance further provides that

> 'For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of "Type 2 surveillance" in subsection (1) is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege will be obtained by carrying it out.'

6.6 As required under section 63 of the Ordinance, the Secretary for Security has issued a Code of Practice ('Code') for ICSO[Note 5] for the purpose of providing practical guidance to law enforcement officers. In the Code there is a further elaboration to distinguish Type 1 surveillance from Type 2 surveillance –

> 'The distinction between Type 1 and Type 2 covert surveillance reflects the different degrees of intrusiveness into the privacy of those who are subject to the surveillance. Type 2 surveillance covers 'participant monitoring' situations where the words or activities of the target of surveillance are being listened to, monitored by or recorded by someone (using a listening device or optical surveillance device) whom the target reasonably expects to be so listening or observing. It also covers situations where the use of an optical or tracking device does not involve entry onto premises without permission or interference with the interior of conveyance or object, or electronic interference with the device, without permission.' (Paragraph 28, Code of Practice for ICSO.)

and

> 'Any covert surveillance which is otherwise Type 2 surveillance is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege (LPP) will be obtained by carrying it out.' (Paragraph 29, Code of Practice for ICSO.)

In view of its more intrusive nature, a Type 1 surveillance operation requires a panel judge's authorization whereas an executive authorization would suffice for Type 2 surveillance [section 8 and section 14].

Note 5 The Code of Practice for ICSO is available from the website of the Security Bureau at <http://www.sb.gov.hk/eng/news/pdfs/cop_e.pdf>.

Judges' authorizations

6.7 Any Type 1 surveillance requires a panel judge's authorization. When applying for issue or renewal of an authorization for Type 1 surveillance, law enforcement officers need to provide sufficient grounds to satisfy the panel judge that the statutory purpose sought to be furthered by the operation concerned has been met and the operation could pass the proportionality test as set out in section 3 of the Ordinance. Only when the panel judge is satisfied that there is no other appropriate less intrusive means to obtain the expected information that an application will be approved. Otherwise the panel judge may refuse the application with expressed reasons.

Maximum approved duration of a judge's authorization

6.8 The Ordinance stipulates that the maximum duration authorized for a Type 1 surveillance application is in any case not to be longer than the period of three months [section 10(b)]. Renewals for the original judge's authorization concerned may be applied for before its expiration. The same maximum duration is also set for a renewed authorization [section 13(b)].

6.9 The longest duration as authorized by the panel judges for Type 1 surveillance for the report period was 14 days. The overall average duration for Type 1 surveillance authorizations granted was only five days.

Emergency authorizations

6.10 If a law enforcement officer of an LEA considers that there is immediate need for Type 1 surveillance due to an imminent risk of death or serious bodily harm, substantial damage to property, serious threat to

public security or loss of vital evidence, and having regard to all the circumstances that it is not reasonably practicable to apply to a panel judge, he/she may apply in writing to the head of his/her department for issue of an emergency authorization for Type 1 surveillance [section 20(1)]. An emergency authorization shall not last for more than 48 hours and may not be renewed [section 22(1)(b) and (2)]. Within the period of 48 hours from the issue of the emergency authorization, the officer is required to apply to a panel judge for its confirmation [section 23(1)].

6.11 No application for emergency authorization for Type 1 surveillance was ever made by LEAs in the report period.

Oral applications

6.12 Basically, all applications for Type 1 surveillance, including applications for emergency authorization, should be made in writing. Notwithstanding this, an application for a prescribed authorization may also be made orally when it is not reasonably practicable to make a written application [section 25]. The relevant authority may deliver his determination orally to issue the prescribed authorization or refuse the application; however, he shall not grant the application unless satisfied that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provisions [section 25(2)]. Such a granted authorization will have the same effect as if an application had been made in writing [section 25(5)].

6.13 The oral application procedure should only be resorted to in exceptional circumstances and in time-critical cases where the normal written application procedure cannot be followed. The Code further

reminds officers that only in urgent circumstances, such as a case involving imminent serious bodily harm without enough time to have the supporting affidavit in writing to be prepared, that an oral application can be justified.

6.14 After obtaining the prescribed authorization by virtue of an oral application, the law enforcement officer concerned is required by the Ordinance [section 26] to as soon as reasonably practicable apply in writing to the relevant authority (a panel judge for Type 1 surveillance) within 48 hours from the issue of the authorization for confirmation of that prescribed authorization. Failing to do so will cause that orally-granted prescribed authorization to be regarded as revoked upon the expiration of the 48 hours.

6.15 During the report period, no oral application for Type 1 surveillance was ever made.

Written applications

6.16 Throughout the report period, a total of 59 written applications were made by LEAs[Note 6]. Only 30 judges' authorizations were granted, of which 29 were made pursuant to fresh applications and one was consequent upon a renewal application. 29 applications were refused. Out of the 29 refused applications, 28 of them were made in the first batch of applications immediately after the passage of the Ordinance.

6.17 The large number of refused applications during the beginning stage of the new regime had aroused my attention. During my inspection visits to the LEAs, I randomly checked the application files of some of the refused applications to see why this had happened. I also requested copies

Note 6 The number of applications granted does not necessarily equal the number of investigation cases. A particular investigation case could involve more than one application for interception / surveillance.

of the reasons given by the panel judges for refusal of all the 28 cases to be provided to me. The refusals were mainly based on the following reasons:

(a) the duration of some of the authorizations sought was too long;

(b) the geographic coverage requested for some authorizations applied for was too wide; and

(c) the affidavit (supporting the application) had not provided sufficient details in support.

6.18 To summarize, the refused applications were considered by the panel judges as too intrusive and disproportionate to the benefits likely to be obtained by the surveillance. I would conclude that the high refusal rate during the first batch of applications was mainly due to the fact that officers did not have sufficient understanding of the new statutory requirements and the standard as held by the panel judges. It is not uncommon that teething problems occur during the early stage of a new regime. Following this batch of refusals, the LEA officers promptly corrected their defects and deficiencies and the situation had significantly improved. There was only one refused application for Type 1 surveillance thereafter till the end of the report period on 31 December 2006.

6.19 While some law enforcement officers may feel that the standard held by the panel judges was too stringent, I consider that the panel judges were justified in striking a fair balance between fighting and detecting serious crimes or protecting public security on the one hand and protection of personal privacy on the other. Officers however should not take the judges' attitude as an unnecessary hindrance to their investigation work. On the contrary, a clear and positive message has in fact been conveyed to the community that each and every application has to pass

through the panel judges' serious and thorough consideration on its appropriateness before it is allowed. The new ICSO regime has given rise to judge-guarded protection of personal privacy against any possible unauthorized surveillance.

Offences

6.20 A list of the major categories of offences for the investigation of which prescribed authorizations for both Type 1 and Type 2 surveillance had been issued or renewed in the report period can be found in Table 2(b) in Chapter 12.

Revocation of authorizations

6.21 For Type 1 surveillance, during the report period there were nine authorizations revoked pursuant to section 57 and one authorization revoked pursuant to section 58.

6.22 As I have mentioned in paragraph 5.20 of Chapter 5, there was no uniform practice among LEAs for revoking prescribed authorizations where a ground for discontinuance arose following arrest (ie, whether it should be done under section 57 – 'discontinuance of interception or covert surveillance' or under section 58 – 'reports to relevant authorities following arrests') (detailed discussions on this issue can be found in paragraphs 11.20 to 11.23 of Chapter 11). The single revocation under section 58 mentioned in the preceding paragraph is one of such examples. The original authorization was a premises-based Type 1 surveillance operation. The LEA concerned took steps to discontinue the operation shortly after the arrest of three persons and report to the PJO by invoking section 58. After going through the contents of the relevant application file, I took the view

that the authorization should be revoked under section 57 as the case officer did not perceive any need to continue with the operation after the arrest. Thus, section 57 should have been engaged. The practice has since been standardized.

Legal professional privilege

6.23 There was no case in which information subject to LPP had been obtained in consequence of any Type 1 surveillance carried out pursuant to prescribed authorizations throughout the report period.

Types of surveillance device

6.24 Section 2(1) of the Ordinance defines a surveillance device as a data surveillance device, a listening device, an optical surveillance device or a tracking device or a combination of any two or more of them. Each authorized surveillance operation, depending on the need of each particular case, may use one or more than one kind of surveillance device. During the report period, most of the surveillance operations conducted involved a composite use of listening and optical surveillance devices.

6.25 It may be noted that I have not broken down the figures into specific types of device or into individual LEAs, for doing so, in my view, may unnecessarily disclose their operation information. Criminals may take advantage from such information when considering the means of communication to be adopted for their criminal activities. For example, if criminals know that a particular LEA conducts relatively more surveillance operations than interceptions, they may choose to rely more on, say, telecommunications communications for contacting and discussing with other associates or gang members. This would adversely affect LEAs in

performing their duties of preventing or detecting criminal activities. For such security or other purposes, I keep the presentation of figures in this report as simple as possible and only where necessary.

6.26 I have developed a scheme whereby I am able to check against possible abuse and to ensure that no LEA would be conducting any surveillance operation without the authority of a prescribed authorization. This scheme was built on the fact that surveillance must be carried out with surveillance devices, especially those that are sophisticated and generally not affordable by officers, that LEAs have the obligation to keep a comprehensive record of such devices and that they are also obliged to keep track of the movement of such devices.

6.27 I started to request the LEAs to develop a comprehensive record system of surveillance devices and also a control mechanism for issuing and collecting them. All surveillance devices are to be stored and managed by a registry, at headquarters/sectional/district office level as may be appropriate. A serial number should be issued to each single surveillance device item, particularly to those more sophisticated items applicable to or specially designed for Type 1 surveillance. The inventory records in each registry should be updated after any addition of new items or deletion of existing items.

6.28 Moreover, the register should record the movement of each loan request, together with the relating prescribed authorization number (ie ICSO No.). The LEAs are obliged to keep track of the movement of surveillance device items. I specifically warned the LEAs that in case of a late return beyond the authorized duration, officers should be required to provide justification or explanation.

6.29 In October 2006, I started to request the LEAs to let me have sight of their registers of surveillance devices. After going through the registers, I made a number of observations and suggested the following improvements:

(a) Some registers did not include the relevant ICSO reference number and the approved duration of the prescribed authorization. Relevant agencies were requested to add such information to the registers for better monitoring purpose. With this information recorded in the registers, it ensures that each loan request is supported by a prescribed authorization. Moreover, it will facilitate my checking if there is any unreasonably late return after the expiry of the authorization. If so, the agency concerned will be requested to explain why this happened and to clarify if any unauthorized surveillance was conducted during the time gap.

(b) I requested LEAs to submit to me copies of inventory lists of surveillance devices being maintained in respective surveillance device registries. Each inventory list should have essential information of each inventory item, including but not limited to serial/inventory number, brand name, type, capability and quantity. These inventory lists should be updated from time to time and submitted to my office on a regular basis. Based on such inventory lists and the registers referred to above, I can have a general picture of what surveillance devices are being used for surveillance and how frequently they are used.

(c) For each registry, separate records should be kept for loan

requests requiring support of a prescribed authorization and loan requests of surveillance devices in respect of which no prescribed authorization is required (such as the use of a video camera to record activities of a subject at a public place) or for administrative or other purposes (such as using a digital camera to take photos of a crime scene for record or evidence purpose).

(d) The description of the loaned items shown in the registers was not to be made complicated so as not to hinder me or my staff in matching such items with the inventory lists. It would be desirable to have cross reference, say an inventory number, indicated in the register to facilitate my examination or inspection.

(e) To prevent loan of surveillance device items that are unnecessary for the operation concerned, the relevant case officer should obtain prior third-party endorsement, preferably from a supervisor, duly signing on the request form.

(f) It would also be desirable if officers could record how the surveillance devices were used or to be used. This will facilitate me, being a layman to such devices and investigation methods, to have a better understanding of how such surveillance devices are used in operation.

6.30 In addition to the above, I plan to make inspection visits, including surprise visits, to the registries to check whether the loaned items correspond to those recorded in the register. Should I find any suspicious case of abuse, I would request a full and detailed explanation from the head

of department concerned. I believe that the above measures will control the use of surveillance devices by the LEAs and better safeguard their compliance with the requirements of the Ordinance.

Effectiveness of surveillance

6.31 Similar to interception, LEAs consider that surveillance, be it Type 1 or Type 2, is an effective and valuable investigation method. During the report period, a total of 50 persons who were subjects of authorized surveillance operations were arrested as a result of or further to such operations. A further 39 non-subjects were also arrested consequent upon the operations. Please see Table 3(b) in Chapter 12.

Checking of cases

6.32 During my periodical inspection visits to the LEAs, as part of the random checking exercise, I had checked the relevant details of 21 applications/related matters for Type 1 surveillance, including those of the granted authorizations and refused applications. Upon my examination, they were all found to be in order and no irregularity of any sort was observed from them.

CHAPTER 7

TYPE 2 SURVEILLANCE

Definition

7.1 Unlike Type 1 surveillance, section 2(1) of the Ordinance gives quite a detailed description of Type 2 surveillance, which is defined as surveillance that –

> '(a) is carried out with the use of a listening device or an optical surveillance device by any person for the purpose of listening to, monitoring or recording words spoken or activity carried out by any other person, if the person using the device –
>
> (i) is a person by whom the other person intends, or should reasonably expect, the words or activity to be heard or seen; or
>
> (ii) listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i); or
>
> (b) is carried out with the use of an optical surveillance device or a tracking device, if the use of the device does not involve –
>
> (i) entry onto any premises without permission; or
>
> (ii) interference with the interior of any conveyance or object, or electronic interference with the device, without permission.'

7.2 In addition, if it is likely that any information which may be subject to LPP will be obtained by carrying out Type 2 surveillance, it is regarded as Type 1 surveillance and law enforcement officers must act accordingly in applying for the issue or renewal of a prescribed authorization [section 2(3)].

Executive authorizations

7.3 An application, fresh or renewed, by a department for a prescribed authorization to carry out Type 2 surveillance may be made to an authorizing officer of the department concerned, who is an officer not

below the rank equivalent to that of senior superintendent of police designated by the head of the department. Such an authorization when granted is called an 'executive authorization' [sections 2 and 14]. Applications for Type 2 surveillance should be made, the same as other applications for interceptions/Type 1 surveillance, in writing [section 14]. Upon consideration of all relevant supporting grounds, the authorizing officer may decide to issue the authorization (with or without variations) or to refuse the application with stated reasons [section 15].

Maximum approved duration of an executive authorization

7.4 The maximum authorized duration for Type 2 surveillance is in any case not to be longer than the period of three months [section 16(b)]. Renewals for the original executive authorization concerned may be applied for before its expiration. The same maximum duration is also set for a renewed authorization [section 19(b)]. For this report period, the longest Type 2 surveillance as authorized lasted 61 days. However, the overall average duration for authorized Type 2 surveillance as a whole, stemming from both written and oral applications, was only 11 days.

Emergency authorization

7.5 Under the Ordinance, unlike Type 1 surveillance, there is no provision by which Type 2 surveillance can be made subject of an application for emergency authorization.

Oral applications

7.6 However, an application for authorization of Type 2 surveillance can be made orally to the authorizing officer [section 25]. For the report period, there were a total of four prescribed authorizations for

Type 2 surveillance granted pursuant to oral applications. No oral application was refused.

Written applications

7.7 Throughout the report period, a total of 46 written applications for Type 2 surveillance were made by the LEAs[Note 7]. 43 executive authorizations were granted, including 35 made pursuant to fresh applications and eight consequent upon renewal applications. Only three applications were refused, mainly for the reason that they did not meet the threshold of immediacy and gravity.

Offences

7.8 A list of the major categories of offences for both Type 1 and Type 2 surveillance can be found in Table 2(b) in Chapter 12.

Revocation of authorizations

7.9 In the report period, in respect of Type 2 surveillance, there were 17 authorizations revoked under section 57 and four authorizations revoked under section 58.

7.10 Similar to Type 1 surveillance, no uniform practice was adopted by LEAs for revoking prescribed authorizations where a ground for discontinuance arose following arrest (ie, whether it should be done pursuant to section 57 or section 58) (detailed discussions on this issue can be found in paragraphs 11.20 to 11.23 of Chapter 11). The revocations under section 58 of the four authorizations mentioned in the preceding

Note 7 The number of applications granted does not necessarily equal the number of investigation cases. A particular investigation case could involve more than one application for interception / surveillance.

paragraph are again, like the Type 1 surveillance revocation case, where section 57 would have been more appropriately invoked.

Legal professional privilege

7.11 There was no case in which information subject to LPP had been obtained in consequence of any Type 2 surveillance carried out pursuant to prescribed authorizations throughout the report period.

Report of irregularity

7.12 In the report period, there was one irregularity reported by the head of an LEA concerning the revocation of a prescribed authorization for Type 2 surveillance. Details of this case can be found in Chapter 10.

Checking of cases

7.13 Although Type 2 surveillance is generally less intrusive than Type 1 surveillance and interception, the entirety of the application procedure for Type 2 surveillance is completed internally within the department. Without the scrutiny of a panel judge, it is important to ensure that all such operations correctly fall within the category of Type 2 surveillance and there is no Type 1 surveillance conducted under the name or guise of Type 2 surveillance. For this reason, I gave much of my attention to checking all the application files in relation to Type 2 surveillance, including granted fresh and renewal authorizations and also refused applications.

7.14 Out of a total of 50 cases relating to Type 2 surveillance for the report period, 33 of the application and related files had been checked in my inspection visits to the LEAs by the end of 2006, while the remaining

of the cases and related files were checked in such visits in 2007. I concluded that all the cases were in order.

Types of surveillance device

7.15 In the report period, most of the Type 2 surveillance operations involved the composite use of listening and optical surveillance devices.

7.16 Regarding the need for a comprehensive inventory list and also a loan register for surveillance devices, what have already been mentioned in paragraphs 6.26 to 6.30 of Chapter 6 above apply to Type 2 surveillance.

7.17 What I would like to add is that the officers-in-charge of the registry should be cautious with respect to each loan request so as to ensure that surveillance devices that meet the needs of the prescribed authorization are issued. Sophisticated devices should not be issued to officers if less sophisticated ones would suffice. In general, if there is a real need to use sophisticated devices for Type 2 purposes or even non-covert surveillance purposes, I would expect detailed and sufficient justification be given and recorded on the loan registers.

Effectiveness of surveillance

7.18 Similar to interception, LEAs consider that surveillance, be it Type 1 or Type 2, is an effective and valuable investigation method. The arrest figures for the report period can be found in Table 3(b) in Chapter 12.

CHAPTER 8

APPLICATION FOR EXAMINATION AND NOTIFICATION TO RELEVANT PERSON

The law

8.1 The Ordinance stipulates that a person may apply to the Commissioner for an examination if he suspects that he is the subject of any interception or surveillance activity that has been carried out by officers of the LEAs. The application is to be made in writing. Save where the circumstances set out in section 45(1) apply, the Commissioner shall, upon receiving an application, carry out an examination to determine:

(a) whether or not the suspected or alleged interception or surveillance has taken place; and

(b) if so, whether or not such interception or surveillance has been carried out by an officer of a department without the authority of a prescribed authorization.

If the Commissioner finds the case in the applicant's favour, he shall notify the applicant and initiate the procedure for awarding payment of compensation to him by the Government.

[Sections 43 and 44.]

8.2 The circumstances provided in section 45(1) that justify the Commissioner not carrying out an examination are that, in the opinion of the Commissioner, the application is received by him more than 1 year after the last occasion on which the suspected interception or surveillance is alleged to have taken place, that the application is made anonymously, that

the applicant cannot be identified or traced after the use of reasonable efforts, and that the application is frivolous or vexatious or is not made in good faith.

The applications under section 45

8.3 During the report period, a total of 19 applications for examination were received. One of these applications was subsequently not pursued by the applicant. Of the remaining 18 applications, five concerned suspected cases of interception and one alleged surveillance. The other 12 related to a combination of both. As the Commissioner, I did not consider that any of the 18 applications came within the ambit of the exceptions covered by section 45(1), and thus I had carried out an examination provided for in section 44 in respect of each case.

The procedure

8.4 The steps taken for such examination can be briefly described as follows. The Commissioner's office will make enquiries with the particular LEA who, as the applicant alleges, has carried out either interception or surveillance activity against him as to whether such a statutory activity had taken place, and if so the reason why. Enquiries will also be made with the PJO as to whether any authorization had been granted by any panel judge for the LEA to carry out any such activity, and if so the grounds for so doing. Where enquiries with any other party may help obtain evidence regarding the existence or otherwise of any such alleged statutory activity, that will also be pursued. The results of the enquiries made will be compared and counterchecked to ensure correctness. Apart from the above information, it is undesirable to disclose more details about the methods used for the examination of applications or about the

examinations undertaken, because that would probably divulge information relating to the prevention or detection of crime or to the protection of public security, which would put LEAs in a disadvantageous position as against criminals or possible criminals.

8.5 Regarding the 18 applications for examination, after making enquiries with the necessary parties, I found all these cases not in the applicants' favour and I notified each of them in writing respectively of my finding accordingly, with 15 of such notices issued during the report period and three thereafter.

8.6 Upon receiving my determination on their cases, six applicants requested me to give reasons for my determination and to indicate whether or not the cases of interception or surveillance that they alleged had taken place. They were all advised that under the Ordinance, the Commissioner was not allowed to provide reasons for his determination or to inform the applicant whether or not the alleged interception or surveillance that was suspected had indeed occurred. The statutory provisions can be found in section 46(4) of the Ordinance.

Section 48 cases

8.7 Another procedure may also result in compensation being awarded by the Commissioner to a person being found to have been subject to an unauthorized interception or surveillance. Under section 48 of the Ordinance, if, in the course of performing any of his functions under the Ordinance, the Commissioner considers that there is any case in which any interception or surveillance has been carried out by an officer of an LEA without the authority of a prescribed authorization, the Commissioner shall, subject to certain exceptions, inform the relevant person of his right to

apply to the Commissioner for an examination in respect of the discovered activity.

8.8 There was a case in which I was apprised of an interception that had taken place without the authority of a prescribed authorization. This was due to the fact that there was an interception of a telephone line that was other than that authorized by a panel judge's authorization. The error was caused by an inadvertent wrong interception of a telephone line instead of intercepting the line authorized by the authorization. However, after having made investigations with the necessary parties, I considered that the person who used the telephone line that had been intercepted without authority could not, despite the use of reasonable efforts, be identified or traced. Thus, the criterion under section 48(6)(a) of the Ordinance for exception having been satisfied, I considered that the requirement for giving notice to the relevant person did not arise. More details of this unauthorized interception can be found in Chapter 10 on irregularities.

8.9 There were two other cases of interception that took place prior to the effective date of the related prescribed authorization. I decided not to give notice pursuant to section 48(1) to the persons affected, mainly for fear that such a notice would be prejudicial to the prevention or detection of crime. Details relating to these two cases can also be found in paragraphs 10.6 to 10.11 of Chapter 10.

8.10 In the result, during this report period, there was no occasion on which the provisions of section 44(3) regarding my making an order for payment of compensation by the Government to any successful applicant

had been invoked and the necessity for my assessing such compensation never arose.

CHAPTER 9

THE CODE OF PRACTICE AND RECOMMENDATIONS TO THE SECRETARY FOR SECURITY

Code of Practice

9.1 Pursuant to section 63 of the Ordinance, a code of practice ('Code') was issued by the Secretary for Security on 9 August 2006. The Code is to provide practical guidance to officers of the LEAs in respect of matters provided for in the Ordinance. The Secretary for Security may in the Code specify the form of any application to be made to a panel judge under the Ordinance. He may from time to time revise the whole or any part of the Code.

9.2 Any officer of an LEA shall, in performing any function under or for the purpose of any provision of the Ordinance, comply with the provisions of the Code. Non-compliance with the Code constitutes non-compliance with the 'relevant requirements' of the Ordinance[Note 8], and has to be reported to the Commissioner. Depending on the circumstances of the case, the relevant officer may be subject to disciplinary action or the common law offence of misconduct in public office, in addition to the full range of existing law.

9.3 The Code sets out practical guidance for the application for the granting of prescribed authorizations in respect of interception and surveillance, defining terms and concepts such as 'private information', 'reasonable expectation of privacy', 'public place', 'necessity and

---

Note 8 'Relevant requirement' means any applicable requirement under any provision of the Ordinance, the code of practice or any prescribed authorization or device retrieval warrant concerned.

proportionality', etc. General rules are laid down in the Code in respect of the procedures to be observed in obtaining and implementing panel judges' authorizations, executive authorizations and emergency authorizations, and in making oral applications. The Code also sets out the functions of the Commissioner and the circumstances under which a report to the Commissioner is required to be made by the LEA concerned.

9.4 A list of prescribed forms to be used in connection with the provisions of the Ordinance together with specimen forms are given at the Annex to the Code (collectively referred to as 'COP forms').

Recommendations to the Secretary for Security

9.5 Under section 51 of the Ordinance, if the Commissioner considers that any provision of the Code should be revised to better carry out the objects of this Ordinance, he may make such recommendations to the Secretary for Security as he thinks fit.

9.6 During the report period, I made a number of recommendations to the LEAs to better carry out the objects of the Ordinance. The Secretary for Security and his staff have been heavily engaged in coordinating the responses from the LEAs and drawing up their implementation proposals. As these recommendations involve changes to the procedures and practices in the implementation and discontinuance of prescribed authorizations and impose additional reporting requirements, they will need to be reflected in the Code to update the procedures and guidelines therein when the Code is next revised. These recommendations are discussed in detail in Chapter 11.

9.7 During the report period, I also reviewed the COP forms annexed to the Code and other internal forms that were produced under the

coordination of the Secretary for Security to facilitate LEA officers' tasks under the Ordinance ('internal forms'). These forms were in use by the LEAs and PJO under different sections of the Ordinance such as the various types of authorizations, affidavits in support of various applications, revocations, records in writing had the oral applications been made in writing, records of determination for oral applications, statements in writing, modification forms and other miscellaneous forms. I made a number of comments on these forms to improve the content and wording. Except otherwise indicated in the paragraphs below, all my comments on the forms were accepted by the Secretary for Security. Where amendments to COP forms are involved, the LEAs would first update their operational forms, while corresponding amendments to the attachments to the Code will be made when the Code is next updated.

9.8 The following illustrate some of the comments and recommendations I made on the forms, which aimed to better reflect the requirements of the Ordinance and avoid ambiguity.

Illustration 1: COP-16, COP-17, COP-18, STA-1 and STA-2

9.9 Where an executive authorization has been granted by an authorizing officer of an LEA to conduct Type 2 surveillance upon an oral application pursuant to section 25 and an application for confirmation of that authorization is required to be made to the authorizing officer under section 26(1) – COP-16 is the form for such an application for confirmation, COP-17 is the form for confirmation whereas COP-18 is the form for refusing to confirm the authorization. COP-16, 17 and 18 state that the application is supported by, inter alia, a statement in writing of the applicant. Internal forms STA-1 and STA-2 are the sample checklists for

LEA officers' reference as to the types of information that may need to be included in the statements in question:

STA-1 : Statement in writing in support of an application for confirmation of an executive authorization for Type 2 surveillance issued upon oral application [section 26(2)(b)(ii)(B)].

STA-2 : Statement in writing in support of an application for confirmation of the renewal of an executive authorization for Type 2 surveillance granted upon oral application [section 26(2)(b)(ii)(B)].

9.10 STA-1 and STA-2 stated in their headings to be under section 26(2)(b)(ii)(B). However, nowhere in these checklists was specified the necessity of disclosing the information previously provided upon the oral application or of such information having to be declared to be true. Although there is a section on 'Applicant's declaration' in STA-1 and STA-2, it falls short of declaring that the information provided in the statement was that provided at the time of the oral application.

9.11 The relevant part of section 26(2)(b)(ii)(B) that deals with application for confirmation of authorization granted upon oral application requires 'a statement in writing made by the applicant setting out all the information provided pursuant to' section 25(3) 'for the purposes of the oral application'.

9.12 The importance of this information that has been provided for the purposes of the oral application is apparent, for section 27(2) provides that the relevant authority shall not confirm the prescribed authorization or

renewal unless he is satisfied that 'the relevant conditions provision' has been complied with in the issue or grant of the prescribed authorization or renewal.

9.13 I therefore recommended to the Secretary for Security that improvement should be made to these STA-1 and STA-2 forms to comply with the requirement of section 26(2)(b)(ii)(B). The Secretary for Security accepted my recommendation.

Illustration 2: AFF-1and COP-9

9.14 Internal form AFF-1 is a sample checklist of information for inclusion in the affidavit in support of an application for an authorization for interception or Type 1 surveillance. It contained a paragraph requiring the applicant to 'specify, if known, whether during the preceding 2 years, there has been any issue/renewal of a prescribed authorization in which the … person [identified in the affidavit aimed to be targeted] has been subjected to interception or covert surveillance, and if so, particulars of such application(s)'.

9.15 It is not reasonably clear whether the wording 'during the preceding 2 years' in AFF-1 should include the period before the commencement of the Ordinance on 9 August 2006. For example, should the applicant state yes or no if there had been telecommunications interception pursuant to an order issued or renewed before the commencement of the Ordinance under section 33 of the Telecommunications Ordinance, Cap 106 [see section 69 of the Ordinance] or if covert surveillance had been undertaken on the targeted person before the commencement of the Ordinance?

9.16 COP-9 which is a statement in writing in support of an application for an executive authorization for Type 2 surveillance also contains a paragraph similar to that of AFF-1.

9.17 The relevant wording in AFF-1 and COP-9 is in accordance with the relevant subparagraph under paragraph (b) in Part 1, Part 2 and Part 3 of Schedule 3 to the Ordinance which requires the applicant to state in the affidavit or statement in writing supporting an application 'whether, **during the preceding 2 years**, there has been any application for the issue or renewal of a prescribed authorization …'. If the Ordinance has already been in force for two years or more, the wording 'during the preceding 2 years' should be clear enough. But as the Ordinance has been in force for less than one year, the question arose as to whether the 2-year period should also cover the period before the commencement of the Ordinance.

9.18 In paragraph 4.13 of Chapter 4, I have recounted a case where the applicant stated in the affidavit in support of the application that 'there has been no issue of any prescribed authorization in which (the subject) has been subject to interception' within the past two years when in fact interception had been carried out against the targeted subject pursuant to an authorization under the former regime. In that case, the panel judge refused the application because he considered that the statement was misleading. To avoid accusation of misleading the panel judge, the applicant should have stated in the affidavit that the targeted person had been subject to interception **within the past two years**, or that the targeted person had not been subject to interception **since the commencement of the Ordinance**.

9.19 It is important that the wording in the form of affidavit should be clear so that applicants know what to fill in. I made the comment to the Secretary for Security that the wording 'during the preceding 2 years' in AFF-1 (and other similar documents) was not reasonably clear. The Secretary agreed to my view above that the 2-year period should start to run from the coming into force of the Ordinance and further pointed out that the reference to 'prescribed authorization' was intended to make it clear that the authorizations in question were authorizations under the Ordinance. He will be happy to further pursue this matter if necessary.

Illustration 3: AFF-6

9.20 Internal form AFF-6 is a sample checklist of information to be included in the affidavit in support of an application for confirmation of an emergency authorization for interception or Type 1 surveillance issued upon oral application. This form requires the applicant to 'verify the factual content provided to the Head of Department under section 20(2)(b), i.e. the requirements specified in Part 1 or Part 2 of Schedule 3 for the authorization of interception or Type 1 surveillance respectively'.

9.21 Section 20(2)(b) refers to a statement in writing made by the applicant in support of an application for emergency authorization. Section 25(3) provides that where an oral application is made, the information required to be provided for the purposes of the application under the relevant document provision may be provided orally (and accordingly any requirement as to the making of any affidavit or statement does not apply). In other words, where an oral application for emergency authorization is made, there might not be any statement in writing under section 20(2)(b).

9.22 I therefore recommended to the Secretary for Security that the wording in the relevant part of AFF-6 should be rephrased as follows: '**state** the factual content provided to the Head of Department under section 20(2)(b) **or section 25(3)**, ie the requirements specified in Part 1 or Part 2 of Schedule 3 for the authorization of interception or Type 1 surveillance respectively **and verify the same**', as there would not be any statement in writing if the information had been provided orally, so as to enable the panel judge to know that the information verified therein was that provided to the head of department at the time of the oral application. My proposed amendments reflect more accurately the requirement provided for in section 28(1)(b)(ii).

9.23 My recommendation was accepted by the Secretary for Security.

Illustration 4: COP-4, COP-5, COP-16, COP-17 and COP-18

9.24 COP-4, COP-5 and COP-16 are application forms for confirmation of prescribed authorization granted upon oral application. COP-17 is the form for confirming an executive authorization granted upon oral application whereas COP-18 is the form for refusing to confirm. In all these forms, it is stated that the application is supported by, inter alia, a record in writing 'containing all the information that would have been provided under the **relevant application provision** had the oral application been made in writing'.

9.25 I recommended that 'relevant application provision' should be amended to read 'relevant **written** application provision' so as to follow the wording of section 26(2)(b)(i) of the Ordinance. This was accepted by the Secretary for Security.

Illustration 5: COP-9

9.26 COP-9 is a checklist of information that may need to be included in the statement in writing in support of an application for an executive authorization for Type 2 surveillance. To assess the intrusiveness of the Type 2 surveillance on any person, the applicant is required to state in paragraph 4(iii)(c) of the form the likelihood that information which may be subject to LPP will be obtained. This is in compliance with the requirements of Part 3 of Schedule 3 to the Ordinance. However, there is a note in this paragraph which reads '**(Note: Explain also why such likelihood exists and what measures will be taken to minimize the likelihood of it occurring.)**'. I recommended to the Secretary for Security that this Note should be deleted, because if it is likely that information which may be subject to LPP would be obtained, the authorization should be sought from a panel judge by treating the Type 2 surveillance as Type 1 surveillance.

9.27 The Secretary for Security agreed with my comment and would make the necessary amendments to COP-9.

Illustration 6: AFF-1, AFF-2, AFF-3, AFF-4, AFF-5 and AFF-6

9.28 These are internal information checklists for affidavits in support of the following applications in respect of interception or Type 1 surveillance - for authorization, for renewal of authorization, for confirmation of an emergency authorization, for confirmation of an authorization issued/renewed upon oral application, and for confirmation of an emergency authorization issued upon oral application. All these affidavit forms ask the applicant to 'assess the likelihood of obtaining

information which may be subject to legal professional privilege, **including the likelihood of obtaining such information following arrests**'.

9.29 I considered that the assessment on the likelihood of obtaining LPP information following arrests was quite unnecessary at this early stage of an application, when an arrest might not even occur. And in any event, this likelihood of obtaining LPP information 'following arrest' is not required in any of the Parts of Schedule 3 to the Ordinance. Nor is it required in COP-9 which is a statement in writing in support of an application for an executive authorization for Type 2 surveillance.

9.30 The Secretary for Security agreed with my recommendation to delete the part on assessment on the likelihood of obtaining LPP information following arrests.

Illustration 7: EMA-1, STA-4, EMA-2 and EMA-3

9.31 Internal form EMA-1 is an application form for confirmation of an emergency authorization for interception or Type 1 surveillance issued upon oral application and STA-4, EMA-2 and EMA-3 are connected internal forms. However, the procedure covered by these forms seems to be that the application is made to the head of department, instead of a panel judge. They appear to serve no practical purpose because such an application for confirmation must be made to a panel judge within 48 hours after the issue of the original authorization [see sections 23(1), 26(1) and 28(1) of the Ordinance]. Paragraph 103 of the Code also states that in normal circumstances only one application for confirmation from the panel judge should be made. There is no clear definition in the Code on the circumstances under which the head of department's confirmation is required.

9.32 I made the above comments to the Secretary for Security who responded that the two-step process should be retained as an option, as it is provided for in the law, so that the head of department's confirmation of the emergency authorization granted upon oral application could be sought in appropriate cases. Moreover, the procedure of seeking the head of department's confirmation of the oral application would still be required even if the covert operations under the emergency authorization have in fact not been carried out. Hence, the forms in question should be retained.

Other issues

9.33 In the course of my review of the COP- and internal forms, issues that are subject to different interpretation surfaced, namely,

(a) Whether a device retrieval warrant needs to be revoked if it is discontinued by the LEA and whether a panel judge has the power to revoke a device retrieval warrant. I recommended to the Secretary for Security that there was a need to request the panel judge to revoke the device retrieval warrant if it was discontinued. This recommendation was not accepted by the Secretary for Security.

(b) Whether a panel judge has the power to impose additional conditions when confirming an emergency authorization. The Secretary for Security considered that the panel judges did not have such power but the panel judges held the opposite view.

The above two issues which are subject to conflicting interpretations are covered in detail in Chapter 13.

CHAPTER 10

REPORTS OF IRREGULARITIES FROM LEAS AND FINDINGS

Reports of irregularities

10.1 During the report period, I received three reports of four incidents of irregularities from heads of LEAs made pursuant to section 54 of the Ordinance. These involve one Type 2 surveillance and three interception cases, as follows:

Case 1	:	Type 2 surveillance Irregularity in revocation of executive authorization.
Cases 2 and 3	:	Interception Interception of telecommunications facilities ahead of the authorized effective date.
Case 4	:	Interception Wrong interception of a telecommunications facility other than that authorized for interception under a prescribed authorization.

10.2 I had reviewed the above irregularities in accordance with section 41(2) and (3) of the Ordinance and notified heads of LEAs concerned of my findings under section 42. My findings were accepted by the LEAs concerned.

Case 1: Incorrect dating of discontinuance in revoking an executive authorization for Type 2 surveillance

10.3 This incident concerns the wrong entry of the date of discontinuance of surveillance by the authorizing officer when he revoked a prescribed authorization for Type 2 surveillance. The surveillance was discontinued following an arrest of three persons. The discontinuance was reported to the authorizing officer who revoked the authorization. In the revocation signed by him, the authorizing officer wrongly stated a date as the date of discontinuance of the surveillance instead of the correct date which was three days after the stated date. The head of the LEA reported the irregularity to me pursuant to section 54 of the Ordinance.

10.4 I made the following findings after conducting a review:

(a) The authorizing officer had entered wrongly the date of discontinuance of the surveillance when he revoked the prescribed authorization.

(b) The mistake was a genuine careless mistake without any ulterior motive. No damage had been caused to anybody.

(c) The head of the LEA had complied with section 54 of the Ordinance to report the irregularity promptly and proposed appropriate follow up action.

10.5 The LEA had advised the authorizing officer concerned to be more careful in entering records. As a preventive measure, the department also implemented a new feature in its database system to alert users on the validity of the dates that have been input. I was satisfied with the follow up action taken.

Cases 2 and 3: Lines intercepted ahead of the authorized effective date

10.6 Section 10(a) of the Ordinance states that a judge's authorization takes effect at the time specified by the panel judge when issuing the judge's authorization. The irregularities in Cases 2 and 3 relate to a breach of section 10(a) in that two telephone lines, one each in two renewed authorizations, were intercepted a few days earlier than the commencement date authorized by the panel judge.

10.7 Two authorizations, hereinafter referred to as AUTH(1) and AUTH(2), had been issued by a panel judge to be valid for 31 days, both expiring on the same date. AUTH(1) authorized the interception of facilities (in this case, telephone lines) A, B and C whereas AUTH(2) authorized the interception of facility D. Four days prior to their expiration, the panel judge granted a renewal of the two authorizations with effect from their common expiry date with facility E added to AUTH(1) and facility F added to AUTH(2), as applied for by the LEA. In other words, interception of the two newly added facilities E and F could only begin immediately after the expiry of the two authorizations (which were renewed). However, the officer (Officer X) responsible for effecting interception mistakenly arranged the interception of facilities E and F to commence on the date when the panel judge granted the renewals, amidst other fresh authorizations also to commence on that day. Another officer (Officer Y) who was responsible for monitoring the two newly added facilities failed to realize the mistake at the material time. It was not until the morning of the third day after the said commencement that the breach was discovered by Officer Y and the interception on facilities E and F was ceased immediately. The interception on facilities E and F re-commenced on the fourth day in accordance with the time specified in the renewed

authorizations. The head of the LEA reported the irregularities to me and proposed a series of follow up actions to prevent recurrence.

10.8 I conducted a review and interviewed the relevant officers. My findings are set out below:

(a) There was unauthorized interception of the two lines for about three days.

(b) The irregularity was due partly to the oversight of Officer X in failing to heed the commencement date of interception of the new or added facilities as authorized in the renewed authorizations amidst a batch of authorizations issued on the same date containing both the renewed authorizations and fresh authorizations.

(c) Officer Y was partly at fault in failing to notice the mistake until the morning of the third day.

(d) The main cause was both officers' mindset resulting from their familiarity with the old practice that fresh authorizations and renewed authorizations all took effect on the date of issue of both kinds of authorizations, which differed from the new practice in which renewed authorizations might defer the commencement of interception to the date when the original authorizations were due to expire instead of the date when the renewed authorizations were issued. Both Officers X and Y had not yet been accustomed to the new practice.

(e) The irregularity was not caused by malice, ill will, or any ulterior motive.

(f) The unauthorized interceptions were conducted only for a

short period of less than three days and were stopped within less than an hour after discovery of the mistake. The intrusiveness of the interceptions concerned on the subject was, in the circumstances, negligible.

(g) The head of the LEA had complied with section 54 of the Ordinance to report the non-compliance by the officers promptly.

10.9 Both Officers X and Y were advised by the management of the LEA to be more careful and alert. I also advised the head of the LEA that all officers in the department involved in the processing of applications and authorizations under the Ordinance be reminded to pay heed to the new practice and correct their mindset referred to in paragraph 10.8(d) above. I also requested the LEA to keep me informed of the progress of the implementation of its proposed actions to improve the procedure for effecting interception to prevent recurrence. These were duly followed up by the LEA.

10.10 Section 48 of the Ordinance stipulates that –

> '(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner … considers that there is any case in which any interception or covert surveillance has been carried out by an officer of a department without the authority of a prescribed authorization, subject to subsection (6), the Commissioner shall as soon as reasonably practicable give notice to the relevant person –
>
> (a) stating that there has been such a case and indicating whether the case is one of interception or covert surveillance and the duration of the interception or covert surveillance; and
>
> (b) informing the relevant person of his right to apply to the Commissioner for an examination in respect of the interception or covert surveillance.
>
> …

(3) Notwithstanding subsection (1), the Commissioner shall only give a notice under that subsection when he considers that the giving of the notice would not be prejudicial to the prevention or detection of crime or the protection of public security.

…

(6) This section does not require the Commissioner to give any notice to a relevant person if –

(a) the relevant person cannot, after the use of reasonable efforts, be identified or traced;

(b) the Commissioner considers that the intrusiveness of the interception or covert surveillance concerned on the relevant person is negligible; or

(c) …'

10.11 Despite my finding of the unauthorized interceptions referred to in paragraph 10.8(a) above, I decided not to give notice pursuant to section 48(1) to the targeted subjects because I considered that the giving of the notice would be prejudicial to the prevention or detection of crime according to section 48(3) and that the intrusiveness of the interceptions concerned on the subjects was negligible according to section 48(6).

Case 4: Wrong interception of a telephone line other than that authorized for interception

10.12 This irregularity was caused by an inadvertent error in wrongly intercepting a telephone line other than that authorized for interception by a prescribed authorization.

10.13 The LEA had obtained a prescribed authorization from a panel judge to intercept a telephone line. In the course of listening to the intercept product, it became apparent to the LEA that the user of the line was not the targeted subject. The LEA suspected that there might have been a wrong interception and caused an enquiry to be made. Meanwhile, the LEA discontinued the interception. Later on the same day, it was confirmed that the person, not an LEA officer, responsible for effecting the

operation pursuant to the prescribed authorization had inadvertently intercepted a line that was not the line authorized for interception but then the problem had been rectified. The LEA reported the discontinuance of the interception to the panel judge the following day on the ground that there was no further value to continue with the interception and the authorization was revoked by the panel judge accordingly. The LEA reported the case to me about two weeks later.

10.14 I conducted a review of the case by examining the relevant documents and interviewing the relevant law enforcement officers. The wrong interception had taken place for seven days before it was discovered and rectified. I considered that I was duty bound to give notice pursuant to section 48(1) of the Ordinance to the relevant affected person stating the duration of the interception and where appropriate consider awarding to him compensation.

10.15 I required the LEA to make all the necessary enquiries in order to find out the line that had been wrongly intercepted with the identity of the relevant person. I also collected first-hand detailed information on the procedure on how this interception operation had been effected.

10.16 Based on my findings, I considered that there was room for improvement in the security measures in effecting interceptions. I requested the Security Bureau to look into this jointly with the LEAs and all concerned parties.

10.17 As mentioned before, I also required that all possible means be used to identify the wrongly intercepted line and its subscriber. Despite efforts made by the LEA and all concerned, the identities of the wrongly intercepted line, its subscriber and user could not be ascertained. Care had

been taken in the investigation of the identities to ensure that parties with no need to know would not be able, through correlation, to get to know that interceptions had been undertaken and would continue to be undertaken.

10.18 I was satisfied that all concerned parties had used reasonable efforts in their investigations as to the identity of the person affected by the erroneous interception, and that the investigations were made in good faith. In the circumstances, I did not require any further investigation to be made, which might risk prejudicing the prevention or detection of crime or the protection of public security by exposing the operational methods of the LEAs.

10.19 I made the following main findings and recommendations –

(a) There was unauthorized interception of a telephone line for seven days. The wrong interception was caused by an inadvertent human error on the part of the person responsible for effecting the interception, who was not an LEA officer. It was not due to the fault of the LEA or any of its officers.

(b) The identity of the subscriber or user of the line wrongly intercepted could not be ascertained after reasonable efforts had been made.

(c) LEAs should be reminded that in case of a wrong interception for whatever reason, the relevant materials relating to the identity of the wrongly intercepted facility and the affected person as well as the duration of the wrong interception should be preserved for the purpose of enabling me to perform my functions under the Ordinance.

(d) The working procedure and security measures in implementing interceptions should be improved to minimize security risk.

(e) The grounds for discontinuance of the interception as reported to the panel judge were that 'there was no further value to continue with the respective interception'. There was no mention of the wrong interception in the report of discontinuance. This was not satisfactory as it would mislead the panel judge into thinking that it was the termination of the interception of the correct facility which had been found to be of 'no value', as opposed to the true reason for the 'no value' due to a wrong line having been intercepted. The LEA should have included the wrong interception in its report of discontinuance to apprise the panel judge of the full picture.

10.20 I decided not to give notice pursuant to section 48(1) because the relevant person could not, after the use of reasonable efforts, be identified according to section 48(6).

10.21 I have notified the LEA of my above findings and recommendations for follow up by the Security Bureau and LEAs. Following from this incident, the Security Bureau had coordinated efforts to put in place measures to minimize wrong interceptions in future. It also reported to me the follow up action it had taken to improve the security measures in implementing interceptions.

10.22 Apart from the above four cases and the incidents referred to in paragraph 13.38 of Chapter 13, no other irregularity or non-compliance was reported or discovered during the report period.

CHAPTER 11

RECOMMENDATIONS TO LEAS MADE UNDER SECTION 52

My function to recommend

11.1 My functions and duties as the Commissioner are clearly defined in section 40 of the Ordinance. With regard to section 40(b)(iv), without limiting the generality of my function of overseeing the compliance by the LEAs and their officers with the relevant requirements of the Ordinance, I may make recommendations to the Secretary for Security and heads of the LEAs as and when necessary. In respect of making recommendations to the LEAs, further elaboration can be found in section 52. Section 52(1) provides that, in the course of performing any of my functions under the Ordinance, if I consider that any arrangements made by any LEA should be changed to better carry out the objects of the Ordinance, I may make such recommendations to the head of the LEA as I think fit. The head of the LEA concerned shall report to me the details of any measures taken (including any disciplinary action taken in respect of any officer) to implement the recommendations, as soon as reasonably practicable or within the period as I have specified when making the recommendations.

11.2 Section 52(3) also confers on me the discretion to refer the recommendations and any other matters I consider fit to the Chief Executive, the Secretary for Justice and any panel judge or any one of them.

11.3 During the report period, I had made seven recommendations to the heads of the LEAs. There was no occasion on which I considered it appropriate to have the recommendations reported straightaway to the

Chief Executive or the Secretary for Justice, although wherever the recommendations concerned the panel judges, I had informed them of the same, so that they were fully apprised of my recommended arrangements well in advance for the LEAs concerned to put in place that would have a bearing on the practice adopted by the LEAs in their applications for prescribed authorizations before the panel judges or in connection therewith. The recommendations appear below.

(1) Reporting of inclusion/cancellation of communications facilities for an interception with the 'reasonably expected to use' clause granted in a prescribed authorization

11.4 Section 29(1)(b)(ii) of the Ordinance provides that a prescribed authorization for telecommunications interception may contain terms that authorize the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, '**or is reasonably expected to use**'. A prescribed authorization with a 'reasonably expected to use' clause is considered by an LEA as empowering it and its officers during the validity of the authorization to add one or more facilities/services to be intercepted insofar as it has obtained sufficient evidence to show that the targeted subject is now found to be using the facilities/services.

11.5 In other words, this clause, when allowed by a panel judge, grants discretion to the LEA and its officers, in the course of an authorized interception operation, to intercept any communication facilities that the targeted subject is found to be using although at the time when the prescribed authorization was sought, no information or evidence of those facilities was yet available. The facility newly added was not one that had

been made known to the panel judge who granted the prescribed authorization. In view of this apparent latitude given to the LEAs by the panel judges, and in order to minimize the degree of intrusiveness to personal privacy, I paid special attention to authorizations granted with this 'reasonably expected to use' clause, to ensure that all relevant additions of facilities were sufficiently justified and no unnecessary or disproportionate intrusion against any persons including the targeted subject would occur.

11.6 I noted that internally within an LEA, the addition or cancellation of any communications facilities could be done with the approval of a senior departmental officer not below the rank equivalent to that of a senior assistant commissioner of police and in accordance with the relevant internal procedures.

11.7 Due to my concern, I took an opportunity to discuss the matter with the Secretary for Security. I was assured that only when it was strictly necessary and serious consideration had been taken that the 'reasonably expected to use' clause would be sought.

11.8 I was, however, told that the LEAs did not report to the panel judges the addition or cancellation of communication facilities. I considered this practice unsatisfactory. I took the view, which was shared by the panel judges, that as a matter of principle, a panel judge's authorization, including interception, was granted upon the condition that the applicant or any other responsible officer of the LEA shall, as soon as practicable, in any event during the validity of the authorization, bring to the attention of the panel judge any material change of circumstances upon which the authorization was granted. Based on this principle, the panel judges and I considered that an addition or even a cancellation of facilities

was a material change of circumstances that ought to be brought to the panel judges' attention as one of the conditions upon which their authorizations were granted. Cancelling a facility was arguably a discontinuance which should be reported under section 57, and that would amount to a material change of circumstances because apparently 'the conditions for the continuance of the prescribed authorization under section 3 are not met' insofar as that facility was concerned (see section 57(7)). Adding a facility, on the other hand, should also amount to a material change of circumstances because, despite the 'reasonably expected to use' clause, the new facility had not specifically come within the consideration of the panel judge when granting the authorization and he should be kept abreast of this new development. I therefore recommended that the LEA should advise the PJO as soon as reasonably practicable whenever such additions or cancellations were made. I also had to consider and devise measures to ensure that I should receive information on all communications facilities added or cancelled, so as to ensure that all facilities intercepted were done with the authority of a prescribed authorization without exception.

11.9 After several rounds of detailed discussions with the panel judges, the Secretary for Security and the LEAs respectively, I recommended the following guidelines to be adopted across the board:

(a) Each specific facility sought for interception should be contained in a separate consecutive schedule in the draft authorization enclosed in an application made by an LEA, ie Schedule 1 for one facility, Schedule 2 for another facility, etc and a panel judge will grant or refuse each individual schedule as he will indicate and initial in the authorization he grants.

On each schedule, the details of the facility should also be stated.

(b) The addition of one or more facilities other than those set out in the schedules is only permissible where the authorization granted by a panel judge is 'subject-based' and contains the 'reasonably expected to use' clause. The importance is the 'reasonably expected to use' clause.

(c) To facilitate distinction, facilities added under an appropriate authorization (as that referred to in (b) above) ('added facilities') should be separately identified.

(d) For the discontinuance (albeit LEAs call it 'cancellation') of a facility in a schedule, regardless of whether the authorization granted by a panel judge is 'subject-based' and contains the 'reasonably expected to use' clause or is 'service-based' or 'premises-based', it should be reported to the panel judges. That may be seen as a 'partial' revocation under section 57.

(e) Where an authorization granted by a panel judge is 'subject-based' and contains the 'reasonably expected to use' clause, the LEA concerned is permitted to add any facility that the targeted subject is reasonably expected to use, because the LEA is given the discretion to do so by this kind of authorization. In such a case, the LEA should keep the PJO informed.

(f) Where an application for an added facility was made but has been refused, the LEA should also keep the PJO informed.

(g) The cancellation of any added facility (as opposed to a

scheduled facility) is not treated as requiring a panel judge's 'partial' revocation. Further, where an entire authorization is revoked subsequently, only all the scheduled facilities not otherwise revoked by the previous 'partial' revocation(s) are revoked.

(h) Any added facility, not previously cancelled, will not need to be revoked by a panel judge's revocation of the authorization, partial or entire, save where the only remaining facility in force is an added facility (ie without any scheduled facility remaining) and it is to be terminated before expiry, when the panel judge will revoke the entire authorization.

(i) At the expiration of an authorization granted by a panel judge that is 'subject-based' and contains the 'reasonably expected to use' clause, the added facilities also expire.

(j) However, any facility in a schedule that was refused when an authorization was granted is not qualified as an added facility, despite the authorization being 'subject-based' and with the 'reasonably expected to use' clause. If the LEA subsequently wishes to intercept such a refused scheduled facility, a fresh application must be made to a panel judge.

(k) All reports made by an LEA on termination or addition of a facility and on the refusal of an application to add a facility should be furnished to the PJO as soon as reasonably practicable.

11.10 The LEAs unanimously accepted and adopted the above recommended guidelines.

(2) Standardization of categorization of interception and surveillance

11.11 There are two kinds of interceptions: postal interception and telecommunications interception. Interceptions can be classified into three forms or a combination of them:

(a) premises/address-based,

(b) service-based, and

(c) subject-based.

11.12 On the other hand, surveillance (Type 1 and Type 2) can be classified into three bases, namely,

(a) premises-based,

(b) object-based, and

(c) subject-based.

11.13 In the weekly reports submitted by LEAs as well as the PJO, I noted that different LEAs had held different views on the categorization of the basis of an interception and surveillance. It was not uncommon that LEAs' categorization did not tally with that of panel judges. I was puzzled as to why this discrepancy could have occurred. Clarifications were sought from relevant parties. Under the prevailing practice at the time, the LEAs submitted their applications for issue of a panel judge's authorization to the PJO with affidavits in support and other supporting documents if necessary. I noted that in most of the affidavits, there was no direct and express mention on the categorization of the operation to be conducted. Similarly, the authorization, the draft of which was also prepared by the LEAs, did not make mention of such classification either. In other words, both sides did not expressly mention in relevant documents the classification of the form of the operation.

11.14 This absence of any expression about the classification of an interception or surveillance in the authorization might lead to a misunderstanding of its scope as approved by the panel judge and, if carried out in a way outside the scope due to the misunderstanding, could lead to an undesirable and disproportionate intrusion upon persons, subjects or non-subjects. For instance, take a case of surveillance, a 'premises-based' surveillance represents that relevant surveillance operation can be targeted at or carried out in particular premises: the activities or conversations of anyone inside the premises could be monitored or recorded by law enforcement officers by the use of listening and optical devices. On the other hand, a 'premises-based and subject-based' surveillance carries a more restrictive meaning. In such case, surveillance operation could be carried out only when the targeted subject, as stated in the authorization, is inside the premises clearly described in it. A different categorization could lead to a different mode of operation and, more importantly, different degree of intrusiveness.

11.15 Moreover, where an LEA classified an interception as 'subject-based', more information on the operation, such as the number of facilities authorized to be intercepted in the case of a telecommunications interception, should also be provided to me. In fact, I opined that such information is important for my review and counter-checking with the relevant parties that only authorized interceptions had been carried out.

11.16 I saw that the problem due to inconsistent categorization of interceptions and surveillance could be eliminated simply by improving the design of the draft authorization. I recommended to the LEAs to revise their affidavit form and the draft authorization form to set out clearly in the

affidavit in support of an application to any panel judge and in the draft authorization the following particulars:

(a) the basis of the interception or surveillance required (eg, 'subject-based', 'service-based' or 'premises-based' or a combination of more than one basis);

(b) the number of communications services involved (for interception);

(c) details of the facility;

(d) whether authorization for 'reasonably expected to use' clause is sought for a telecommunications interception; and

(e) whether LPP information or journalistic material may be involved.

11.17 If the panel judge approves the application concerned but holds different views on some aspects, he may reflect his views by simply making corresponding amendments on the draft authorization authenticating them with his initials when he signs the authorization. The panel judge's authorization and the particulars contained in it should be the basis for the operation and also for filling in the weekly returns to be furnished to me.

11.18 I also issued guidelines on the categorization –

(a) Where an authorization for telecommunications interception is confined to the facility set out in the schedule(s) attached to the authorization without the 'reasonably expected to use' clause, this should be classified as 'service-based'.

(b) Where an authorization for telecommunications interception contains the 'reasonably expected to use' clause, this should be classified as 'subject-based'.

(c) Where an interception or surveillance is classified by a panel judge as 'subject-based and premises-based', the authorization is to the effect that the authorized activity must be directed at the targeted subject at the specified premises. The premises specified is a limitation of the subject-based authorization and not an alternative that the operation could either be carried out as against the subject generally or at the specified premises.

(d) The fact that an original authorization for interception of telecommunications contained the 'reasonably expected to use' clause and that the same discretion was requested by the LEA in its application for renewed authorization does not necessarily mean that the same would be granted in the renewed authorization unless the panel judge has expressly stated the 'reasonably expected to use' clause in the renewed authorization.

11.19 My above recommendations had been accepted and implemented across the board.

(3) Uniform and proper use of sections 57 and 58

11.20 Section 57 of the Ordinance provides that if the officer concerned, during an operation of interception or surveillance, is of the opinion or becomes aware that the ground for discontinuance of a prescribed authorization exists, he shall, as soon as reasonably practicable thereafter, cause the interception or surveillance to be discontinued. On the

other hand, section 58 provides that when the officer becomes aware that the subject of the interception or surveillance has been arrested, the officer shall, as soon as reasonably practicable, cause to report to the relevant authority. In the report, he should assess the effect of the arrest on the likelihood that any information which may be subject to LPP will be obtained by continuing the interception or surveillance.

11.21 I noticed that different LEAs had different practices for revocation of a prescribed authorization as to whether it should be revoked under section 57 'discontinuance of interception or covert surveillance' or section 58 'reports to relevant authorities following arrests'. There was no uniform application among the LEAs.

11.22 In my view, which was also the consensus of the panel judges, whenever the officer concerned forms an opinion that the interception/surveillance should be discontinued or actually discontinues the operation, a report under section 57 should be made as soon as reasonably practicable to the relevant authority who shall revoke the authorization. This is irrespective of whether an arrest has been made. But where there is an arrest, the arrest has to be stated in the report on discontinuance under section 57 as the basis or part of the basis for the discontinuance. It is only where there is still a requirement of continuance of the operation after an arrest that section 58 should be engaged. A report under section 58 should state the assessment of 'the effect of the arrest on the likelihood that any information which may be subject to legal professional privilege will be obtained by **continuing** the interception or covert surveillance'.

11.23 I recommended the above view to the LEAs, who accepted and adopted the same in practice.

(4) Prompt discontinuance under section 57

11.24 All applications for authorization from LEAs to panel judge are subject to the general rule that the applicant should make full and frank disclosure of all relevant matters. Thus all relevant material should be disclosed by the LEAs. Under this principle, if an authorization granted by a panel judge was simply allowed to lapse, without earlier discontinuance (thus the need to report on discontinuance does not arise), this fact may adversely affect any subsequent application for interception/surveillance relating to the same targeted subject because it might be considered that the lapsed authorization had not been useful and therefore quite unnecessary, contrary to the condition of necessity required by section 3 of the Ordinance.

11.25 I recommended and the LEAs accepted that prompt discontinuance should be made if it is found that the operation is not productive and will no longer be expected to be productive. This should not wait until the natural expiration of the authorization. On the other hand, full and frank disclosure of the lapsed authorization and reasons for allowing it to lapse, instead of discontinuance, should be provided to the panel judge (or the authorizing officer in the case of Type 2 surveillance) in any subsequent application.

(5) Report of revocation of emergency authorization to panel judge

11.26 Section 57(3) provides that a report on the discontinuance shall be made to 'the relevant authority' to whom an application for the

issue or renewal of the prescribed authorization concerned has last been made. The relevant authority shall under section 57(4) revoke the prescribed authorization concerned. Section 58(1) provides that a report assessing the effect of an arrest on the likelihood of obtaining LPP information by continuing the operation shall be made to 'the relevant authority' by whom the prescribed authorization has been issued or renewed. The relevant authority shall under section 58(2) determine whether to revoke the prescribed authorization.

11.27 In case of an emergency authorization granted by the head of department pursuant to section 21, which has been confirmed by a panel judge under section 24(1)(a) and (5)(a), I recommended that the relevant authority to whom a report under section 57(3) or section 58(1) shall be made should be the panel judge, regardless of whether a report will also be made to the head of department. The principle is that insofar as a panel judge's authorization or confirmation has been obtained by the LEA, the report of discontinuance/cancellation or arrest must be made to him. This principle should be applied across the board. It follows that the relevant authority to revoke under section 57(4) or to determine whether to revoke under section 58(2) should also be the panel judge.

11.28 On this issue, the LEAs held a different view. They interpreted that 'relevant authority' would not necessarily be the panel judge. In relation to application for emergency authorization, in their view, the head of department was the relevant authority to approve/refuse the application. They opined that the panel judges were not the relevant authority to revoke emergency authorization.

11.29 The LEAs claimed, however, that in view of their nature emergency authorizations would be very small in number. Also given their very short duration (not more than 48 hours), the probability that an arrest is made or discontinuance is required within the validity of the emergency authorizations would be rare. Moreover, in cases where the LEAs consider it necessary for the operation under an emergency authorization to continue beyond the 48 hours, the LEAs will likely make fresh applications to the panel judges at the same time as they seek confirmation of the emergency authorizations.

11.30 Despite their own view on the subject, the LEAs were agreeable to keep the panel judges informed should sections 57 or 58 be engaged for the revocation of emergency authorizations.

(6) Regular report on number of facilities being intercepted

11.31 It is important to ensure that all interceptions concerned are only those conducted pursuant to a prescribed authorization and no unauthorized interception occurs. In the performance of my functions under the Ordinance, I noted that once they obtained the necessary prescribed authorizations, the LEAs had the assistance of the Team (referred to in paragraph 4.9 of Chapter 4) and (if necessary) CSPs in the conduct of interception. Due to their high degree of sensitivity, these operations were and still are conducted under strict confidentiality.

11.32 To ensure no unauthorized interception operation is done against anyone in Hong Kong, there is a need to keep track on the number of facilities being intercepted by the LEAs. This will need to be checked against the number of facilities the interception of which is authorized by prescribed authorizations. I recommended and required the LEAs and

CSPs to furnish me with regular reports on the respective number of facilities being intercepted by/as known to them as at a particular point of time. Upon the receipt of their reports, detailed comparison studies will be conducted to ensure that the numbers of facilities reported by different parties tally and are consistent, and the interceptions were all covered by prescribed authorizations. Should I find any discrepancy, I would expect a full and frank explanation from LEAs concerned.

(7) Regular submission of inventory list of surveillance devices

11.33 To allow me to check that all surveillance operations are conducted pursuant to prescribed authorizations, I recommended and each LEA agreed to furnish me with an inventory list of all the surveillance devices for surveillance authorized under the Ordinance that the LEA possesses at any given time. In addition, the list should also explain the capability and show the trade or brand name or common name of each device under the categories of –

(a) data surveillance device,

(b) listening device,

(c) optical surveillance device,

(d) tracking device, and

(e) device that is a combination of two or more of the above.

11.34 At the same time I requested each LEA to keep a register (or more than one if circumstances so require) of surveillance devices recording, inter alia, the following particulars, namely,

(a) ICSO No.,

(b) date of expiration of the authorization related to the ICSO No.,

(c) devices concerned,

(d) date and time of issue of the devices, and

(e) date and time of return of the devices.

11.35 I have also suggested that consideration be given to recording the movement of devices capable of being employed for surveillance which are to be used for purposes other than the statutory activities under the Ordinance. This will ensure that any issue of the devices to any officer of the LEA will be duly recorded, facilitating checking and deterring any unauthorized use of such devices.

11.36 Moreover, I have also advised the LEAs that officers-in-charge of the surveillance device registries should pay attention to the expiry date of each and every authorization so as to ensure that loaned items will be returned before the expiry of the authorization concerned and there is no outstanding items kept in officers' hands after the expiry of authorization.

11.37 Other details relating to this recommendation can be found in paragraphs 6.26 to 6.30 of Chapter 6.

Conclusion

11.38 The Ordinance is the first attempt by all concerned to formalize and provide a comprehensive legal basis for the investigation acts of interception and surveillance to be carried out by LEAs for the purposes of prevention and detection of crime or protection of public security. A number of issues arose during the performance of my functions as the oversight authority appointed pursuant to the Ordinance, and whenever I saw the need I had made recommendations to the LEAs so that

improvements to the arrangements already set in place by them and the Security Bureau could be improved. All concerned in the operation of the Ordinance will doubtless discover more issues to be resolved and areas to be improved as time progresses. This is an on-going process that has to and will continue.

CHAPTER 12

STATUTORY TABLES

12.1 In accordance with section 49(2), this chapter appends separate statistical information in relation to interception and surveillance for the report period, covering the commencement of the Ordinance (ie 9 August 2006) and ending on 31 December 2006. The information is set out in table form and comprises the following tables:

(a) Table 1(a) – interception – number of authorizations issued / renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)];

(b) Table 1(b) – surveillance – number of authorizations issued / renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)];

(c) Table 2(a) – interception – major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under the Ordinance [section 49(2)(b)(i)];

(d) Table 2(b) – surveillance – major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under the Ordinance [section 49(2)(b)(i)];

(e) Table 3(a) – interception – number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)];

(f) Table 3(b) – surveillance – number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)];

(g) Table 4 – interception and surveillance – number of device retrieval warrants issued and number of applications for the issue of device retrieval warrants refused [section 49(2)(c)(i) and (ii)];

(h) Table 5 – summary of reviews conducted by the Commissioner under section 41 [section 49(2)(d)(i)];

(i) Table 6 – number and broad nature of cases of irregularities or errors identified in the reviews [section 49(2)(d)(ii)];

(j) Table 7 – number of applications for examination that have been received by the Commissioner [section 49(2)(d)(iii)];

(k) Table 8 – respective numbers of notices given by the Commissioner under section 44(2) and section 44(5) further to examinations [section 49(2)(d)(iv)];

(l) Table 9 – number of cases in which a notice has been given by the Commissioner under section 48 [section 49(2)(d)(v)];

(m) Table 10 – broad nature of recommendations made by the Commissioner under sections 50, 51 and 52 [section 49(2)(d)(vi)];

(n) Table 11(a) and (b) – number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or surveillance carried out pursuant to a prescribed authorization [section 49(2)(d)(vii)]; and

(o) Table 12 – number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 42, 47, 52 or 54 and the broad nature of such action [section 49(2)(d)(viii)].

Interception – Number of authorizations issued / renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)] [Note 9]

Table 1(a)

		Judge's Authorization	Emergency Authorization
(i)	Number of authorizations issued	301	0
	Average duration[Note 10]	30 days	-
(ii)	Number of authorizations renewed	148	Not applicable
	Average duration of renewals	30 days	-
(iii)	Number of authorizations issued as a result of an oral application	0	0
	Average duration	-	-
(iv)	Number of authorizations renewed as a result of an oral application	0	Not applicable
	Average duration of renewals	-	-
(v)	Number of authorizations that have been renewed during the report period further to 5 or more previous renewals	0	Not applicable
(vi)	Number of applications for the issue of authorizations refused	30	0
(vii)	Number of applications for the renewal of authorizations refused	5	Not applicable
(viii)	Number of oral applications for the issue of authorizations refused	0	0
(ix)	Number of oral applications for the renewal of authorizations refused	0	Not applicable

Note 9 Executive authorization is not applicable to interception.

Note 10 The average duration is arrived at by dividing the sum total of the duration of all cases under a category by the number of cases under the same category. The same formula is also used to work out the 'average duration' in Table 1(b).

Surveillance - Number of authorizations issued / renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)]

Table 1(b)

		Judge's Authorization	Executive Authorization	Emergency Authorization
(i)	Number of authorizations issued	29	35	0
	Average duration	5 days	11 days	-
(ii)	Number of authorizations renewed	1	8	Not applicable
	Average duration of renewals	14 days	10 days	-
(iii)	Number of authorizations issued as a result of an oral application	0	4	0
	Average duration	-	8 days	-
(iv)	Number of authorizations renewed as a result of an oral application	0	0	Not applicable
	Average duration of renewals	-	-	-
(v)	Number of authorizations that have been renewed during the report period further to 5 or more previous renewals	0	0	Not applicable
(vi)	Number of applications for the issue of authorizations refused	28	3	0
(vii)	Number of applications for the renewal of authorizations refused	1	0	Not applicable
(viii)	Number of oral applications for the issue of authorizations refused	0	0	0
(ix)	Number of oral applications for the renewal of authorizations refused	0	0	Not applicable

Interception – Major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under the Ordinance [section 49(2)(b)(i)]

Table 2(a)

Offence	Chapter No.	Ordinance
Trafficking in dangerous drugs	Cap 134	Section 4, Dangerous Drugs Ordinance
Managing a triad society	Cap 151	Section 19(2), Societies Ordinance
Arson	Cap 200	Section 60, Crimes Ordinance
Offering advantage to public servant and accepting advantage by public servant	Cap 201	Section 4, Prevention of Bribery Ordinance
Agent accepting advantage and offering advantage to agent	Cap 201	Section 9, Prevention of Bribery Ordinance
Theft	Cap 210	Section 9, Theft Ordinance
Robbery	Cap 210	Section 10, Theft Ordinance
Handling stolen property	Cap 210	Section 24, Theft Ordinance
Conspiracy to inflict grievous bodily harm	Cap 212	Section 17, Offences against the Person Ordinance

Surveillance – Major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under the Ordinance [section 49(2)(b)(i)]

Table 2(b)

Offence	Chapter No.	Ordinance
Dealing with goods to which the Dutiable Commodities Ordinance applies	Cap 109	Section 17(1), Dutiable Commodities Ordinance
Trafficking in dangerous drugs	Cap 134	Section 4, Dangerous Drugs Ordinance
Conspiracy to commit an offence	Cap 200	Section 159A, Crimes Ordinance
Offering advantage to public servant and accepting advantage by public servant	Cap 201	Section 4, Prevention of Bribery Ordinance
Agent accepting advantage and offering advantage to an agent	Cap 201	Section 9, Prevention of Bribery Ordinance
Misconduct in public office	--	Common law

Interception – Number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]

Table 3(a)

	Number of persons arrested[Note 11]		
	Subject	**Non-subject**	**Total**
Interception	59	71	130

Surveillance – Number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]

Table 3(b)

	Number of persons arrested[Note 12]		
	Subject	**Non-subject**	**Total**
Surveillance	50	39	89

Note 11 Of the 130 persons arrested, 42 were attributable to both interception and surveillance operations that had been carried out.

Note 12 Of the 89 persons arrested, 42 were attributable to both interception and surveillance operations that had been carried out. The total number of persons arrested under all statutory activities was in fact 177.

Interception and surveillance - Number of device retrieval warrants issued and number of applications for the issue of device retrieval warrants refused [section 49(2)(c)(i) & (ii)]

Table 4

(i)	Number of device retrieval warrants issued	0
	Average duration	-
(ii)	Number of applications for device retrieval warrants refused	0

Summary of reviews conducted by the Commissioner under section 41 [section 49(2)(d)(i)]

Table 5

Number of reviews conducted under		Interception / Surveillance	Summary of reviews
Section 41(1) Reviews on compliance by departments and their officers with relevant requirements, as the Commissioner considers necessary			
(a) Regular reviews on weekly reports	76	Interception & Surveillance	LEAs are required to submit weekly reports to the Commissioner providing relevant information on authorizations obtained, applications refused and operations discontinued in the preceding week, for the Commissioner's checking and review purposes. During the report period, a total of 76 weekly reports were submitted by the respective LEAs.
(b) Periodical inspection visits to LEAs	8	Interception & Surveillance	In addition to the checking of weekly reports, the Commissioner had paid eight visits to LEAs during the report period. During the visits, the Commissioner conducted detailed checking on the affidavits of doubtful cases as he identified from the weekly reports. Moreover, random inspection of other cases would also be made. Whenever he considered necessary, the Commissioner would seek clarification or explanation from LEAs directly. From the said eight visits, a total of 192 applications/related matters had been checked.

Number of reviews conducted under		Interception / Surveillance	Summary of reviews
Section 41(2) The Commissioner shall conduct reviews on cases in respect of which a report has been submitted to him under section 23(3)(b), 26(3)(b)(ii) or 54			
(a)	Report submitted under section 23(3)(b) by the head of department to the Commissioner on cases in default of application being made for confirmation of emergency authorization within 48 hours	Nil	Not applicable	For the report period, there was no report submitted under this category.
(b)	Report submitted under section 26(3)(b)(ii) by the head of department to the Commissioner on cases in default of application being made for confirmation of prescribed authorization or renewal issued or granted upon oral application within 48 hours	Nil	Not applicable	For the report period, there was no report submitted under this category.
(c)	Report submitted under section 54 by the head of department to the Commissioner on any case of failure by the department or any of its officers to comply with any relevant requirement	3	Surveillance	Report 1 An authorizing officer had entered an incorrect date of discontinuance of Type 2 surveillance when he revoked a prescribed authorization. The Commissioner conducted a review on this case and accepted that it was a genuine careless mistake made by that authorizing officer. The LEA concerned had also complied with section 54 to report this irregularity promptly and had taken appropriate follow-up remedial actions. Having considered that no damage had been caused to anybody by this mistake, the Commissioner concluded that no further action would be required from himself on this case.

Number of reviews conducted under		Interception / Surveillance	Summary of reviews
		Interception	Report 2 (involving two cases) A breach of section 10(a) of ICSO was reported in that two telephone lines, one each in two renewed authorizations, were intercepted earlier than the effective time of the authorizations concerned. At the time when this mistake was discovered, a period of nearly three days of unauthorized interceptions had been conducted. The Commissioner reviewed these two cases and found that the irregularity was mainly due to officers having not yet been accustomed to the new ICSO practice and was not caused by any malice, ill will or ulterior motive. The unauthorized interceptions were stopped within less than an hour after discovery of the mistake. The Commissioner was satisfied that appropriate follow-up action had been taken to prevent recurrence of such mistake in future. Notwithstanding the unauthorized interceptions, the Commissioner decided not to give notice pursuant to section 48(1) to the targeted subjects as he considered that the giving of the notice would be prejudicial to the prevention or detection of crime according to section 48(3) and that under the circumstances the intrusiveness of the interceptions was negligible according to section 48(6).
		Interception	Report 3 It was reported that one telephone line had been wrongly intercepted for an

Number of reviews conducted under		Interception / Surveillance	Summary of reviews
			interception pursuant to a prescribed authorization. The following were the main findings and recommendations: (a) There was unauthorized interception of a telephone line by reason of wrong interception for seven days, caused by an inadvertent human error on the part of a person responsible for effecting the interception (not due to the fault of the LEA or any of its officers). (b) The identity of the subscriber or user of the wrongly intercepted line could not be ascertained after reasonable efforts had been made. (c) LEAs should be reminded that in case of a wrong interception, the relevant materials relating to the identity of the wrongly intercepted facility and the affected person as well as the duration of the wrong interception should be preserved. (d) The working procedure and security measures in implementing interceptions should be improved to minimize security risk. (e) The LEA should have included the wrong interception in its report of discontinuance to apprise the panel judge of the full picture.

Number and broad nature of cases of irregularities or errors identified in the reviews [section 49(2)(d)(ii)]

Table 6

Number of cases of irregularities or errors identified in the reviews under		Interception / Surveillance	Broad nature of irregularities or errors identified
Section 41(1)			
Reviews during the periodical inspection visits to LEAs		Interception & Surveillance	During the interim period between the revocation of a prescribed authorization as a result of a report of arrest under section 58 and the notification of that revocation to the person carrying out the statutory activity, the statutory activity may be unauthorized (see paragraphs 13.34 to 13.44 of Chapter 13 for details). This was discovered during an inspection visit to an LEA in late March 2007.
Section 41(2)			
(a) Reviews on cases in default of application being made for confirmation of the emergency authorization within 48 hours as reported by the head of department under section 23(3)(b)	Nil	Not applicable	As mentioned in Table 5 above, there was no report submitted under this category.
(b) Reviews on cases in default of application being made for confirmation of prescribed authorization or renewal issued or granted upon oral application within 48 hours as reported by the head of department under section 26(3)(b)(ii)	Nil	Not applicable	As mentioned in Table 5 above, there was no report submitted under this category.
(c) Reviews on non-compliance cases as reported by the head of department under section 54	4	Surveillance	Case 1 Wrong entry of the date of the discontinuance of the surveillance in revocation of an executive authorization.

Number of cases of irregularities or errors identified in the reviews under		Interception / Surveillance	Broad nature of irregularities or errors identified
		Interception Interception	Case 2 and Case 3 Unauthorized interception of two telephone lines ahead of the authorized commencement date of two renewed authorizations. Case 4 Wrong interception of a telephone line for an interception pursuant to a prescribed authorization. [For details see Table 5 and Chapter 10.]

Number of applications for examination that have been received by the Commissioner [section 49(2)(d)(iii)]

Table 7

Number of applications received Note 13	Applications for examination in respect of			
	Interception	Surveillance	Both Interception and Surveillance	Case could not be processed
19	5	1	12	1

Note 13 Of the 19 applications received, one application could not be further processed as the applicant had not given a formal consent to the Commissioner to use his particulars for processing the examination.

Respective numbers of notices given by the Commissioner under section 44(2) and section 44(5) further to examinations [section 49(2)(d)(iv)]

Table 8

Number of notices to applicants given by the Commissioner		**Nature of applications for examination**		
		Interception	**Surveillance**	**Both Interception and Surveillance**
Number of cases that the Commissioner had found in the applicant's favour [section 44(2)]	0	-	-	-
Number of cases that the Commissioner had not found in the applicant's favour [section 44(5)][Note 14]	18	5	1	12

Note 14 As mentioned in Note 13 above, there was one application for examination that could not be processed. Therefore the number of notices given by the Commissioner under section 44(5) is 18 instead of 19, 15 of which were given during the report period and three thereafter.

Number of cases in which a notice has been given by the Commissioner under section 48 [section 49(2)(d)(v)]

Table 9

	Number of cases in which a notice has been given in relation to	
	Interception	**Surveillance**
Notice to the relevant person by the Commissioner stating that he considers that there has been a case of interception or surveillance carried out by an officer of a department without the authority of a prescribed authorization and informing the relevant person of his right to apply for an examination [section 48(1)]	0	0

Broad nature of recommendations made by the Commissioner under sections 50, 51 and 52 [section 49(2)(d)(vi)]

Table 10

Recommendations made by the Commissioner		Interception / Surveillance	Broad nature of recommendations
Reports to the Chief Executive on any matter relating to the performance of the Commissioner's functions [section 50]	Nil	Not applicable	Not applicable
Recommendations to the Secretary for Security on the Code of Practice [section 51]		Interception & Surveillance	(1) Recommendations to LEAs on changes to the procedures and practices in the implementation and discontinuance of prescribed authorizations and additional reporting requirements necessitating corresponding changes to the Code of Practice to update the procedures and guidelines therein. (2) Improvement of the wording and content of the COP- and internal forms in use by LEAs and PJO to better reflect the requirements of ICSO and avoid ambiguity.
Recommendations to departments for better carrying out the objects of the Ordinance or the provisions of the Code of Practice [section 52]	7	Interception Interception & Surveillance Interception & Surveillance	(1) Panel judges should be informed whenever there is addition or cancellation of communications facilities under a prescribed authorization. (2) The categorization of the basis of an interception and surveillance should be standardized between panel judges and LEAs. (3) A uniform practice should be set up among LEAs to revoke a prescribed authorization under section 57 'Discontinuance of interception or covert surveillance' or to seek continuation under section 58

Recommendations made by the Commissioner		Interception / Surveillance	Broad nature of recommendations
			'Reports to relevant authorities following arrests'.
		Interception & Surveillance	(4) LEAs were to make prompt discontinuance under section 57 if it was found that the operation was not productive and would no longer be expected to be productive.
		Interception & Surveillance	(5) For revocation of emergency authorization under section 57 or section 58, panel judges should be informed.
		Interception	(6) For the purpose of enabling the Commissioner to check that all interceptions made were only those conducted pursuant to a prescribed authorization, LEAs were required to provide information of the facilities that were being so intercepted on a fixed date and on a regular basis to the Commissioner for checking and reviewing purposes.
		Surveillance	(7) For the purpose of enabling the Commissioner to check that all surveillance operations were conducted pursuant to a prescribed authorization, LEAs were required to compile and keep inventory list of surveillance devices and registers (of withdrawals and returns) of surveillance devices for checking by the Commissioner.

Number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or surveillance carried out pursuant to a prescribed authorization [section 49(2)(d)(vii)]

Table 11(a)

	Number of cases
Interception	0

Table 11(b)

	Number of cases
Surveillance	0

Number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 42, 47, 52 or 54 and the broad nature of such action [section 49(2)(d)(viii)]

Table 12

	Number of cases	**Interception / Surveillance**	**Broad nature of disciplinary action**
Disciplinary action taken as a result of the findings of the Commissioner in a review on compliance by departments under section 41(3) [section 42]	0	Not applicable	Not applicable
Disciplinary action taken to address any issues arising from the determination on an examination made by the Commissioner referred to in section 44(2) [section 47]	0	Not applicable	Not applicable
Disciplinary action taken as a result of recommendations made by the Commissioner for better carrying out the objects of the Ordinance or the provisions of the Code of Practice [section 52]	0	Not applicable	Not applicable
Disciplinary action taken in case of report on non-compliance [section 54]	0	Not applicable	Not applicable

12.2 In accordance with section 49(2)(e), I am required to give an assessment on the overall compliance with the relevant requirements during the report period. Such assessment and the reasons in support can be found in paragraphs 4.11 to 4.20 of Chapter 4.

CHAPTER 13

OTHER REVIEW AND RECOMMENDATIONS

Introduction

13.1 This chapter deals with my review of the provisions of the Ordinance and the practical aspects of its operation in the light of my experience obtained during the report period and thereafter, covering not only the report period but right up to the time of the writing of this report. The justification for going beyond the report period is that the earlier my review and recommendations are known, the sooner improvements can be considered and, if deemed appropriate, carried out.

13.2 The review under this chapter, with the recommendations consequent upon the review, is quite different from the review over the LEAs to ensure compliance by them and their officers with the requirements of the Ordinance, which has been covered by other chapters of this report.

Review and recommendations

13.3 There are a number of the provisions of the Ordinance that are subject to different interpretations. During my consultations with the panel judges, the Security Bureau and the LEAs in the performance of my functions as the Commissioner, I have discovered that the following are so subject, namely,

(a) the power of a panel judge to partially revoke the authorizations that have been granted;

(b) the ambit of coverage of telecommunications facilities that the targeted subject is 'reasonably expected to use' stated in the prescribed authorization granted by a panel judge and the related necessity or otherwise of reporting to the panel judge the fact where there is a facility additionally intercepted under the authorization;

(c) the power of a panel judge to impose additional conditions when confirming an emergency authorization;

(d) the power of a panel judge to revoke a device retrieval warrant; and

(e) section 53 in regard to the Commissioner's power and entitlement to request the panel judges to provide him with copy documents in the due performance of his functions.

13.4 Moreover, there are matters that are not expressly covered by the provisions of the Ordinance, which have given rise to conflicting interpretations and different ways of understanding of what is to be done. There are also practical difficulties regarding the application of section 58 of the Ordinance. A part of section 49 should also be rephrased when the Ordinance is reviewed and amended.

(1) Partial revocation of authorization

13.5 The most blatant difference relates to the situation where a prescribed authorization granted by a panel judge authorized interception of more than one communication service, such as two or three telephone lines, and during the currency of the authorization, the LEA concerned dropped the interception of one of the services. The panel judges adopted the stance that since they had granted the prescribed authorization, insofar as any

service that was authorized to be intercepted was dropped, that would properly result in their having to revoke the authorization partially. However, the LEAs (with the Security Bureau sharing their view) were of the opinion that such a situation did not require the partial revocation of the authorization: they were merely cancelling one of the services in respect of which interception had been authorized. According to their understanding, the Ordinance does not provide for partial revocation of authorizations, and if an authorization is to be revoked, it must be revoked in its entirety. On the other hand, the panel judges were of the view that the power conferred by the Ordinance on them to grant an authorization must include the power to revoke it and to revoke it partially.

13.6 As far as I am concerned, the construction taken by either the panel judges or the LEAs did not affect the performance of my functions to oversee the compliance with the requirements of the Ordinance, so long as clear information was to be provided to me as to the number of services authorized for interception and the number of those cancelled or dropped. I have to keep a vigilant eye so that unauthorized interception or surveillance does not take place, and keeping track of the number of services remaining to be intercepted is an important tool to achieve this aim. There was one matter, however, that required my intervention, which was that the LEAs considered that in the case of the dropping of a service, they did not even need to inform the PJO. I considered this undesirable, to say the least, for the panel judge who granted the authorization should be notified where a portion of the authorization was no longer to be used. Accordingly, I advised all LEAs that a report had to be made to the PJO in case any service under an authorization granted by a panel judge had been dropped even though other portions of the authorization were still being afoot.

13.7 The different views of construction held by the panel judges and by the LEAs can be resolved by the legislature when it takes steps to revise the provisions of the Ordinance in the future.

(2) Interception: telecommunications service that a subject is reasonably expected to use

13.8 The procedure for adding facilities to a prescribed authorization in respect of telecommunications interceptions with the approval of a departmental officer not below the rank equivalent to a senior assistant commissioner of police ('departmental approving officer') is envisaged by paragraph 107 of the Code of Practice issued by the Secretary for Security. This is based on section 29(1)(b)(ii) of the Ordinance and the wording of the authorization to permit interception of a communications service that the targeted subject is 'reasonably expected to use'. However, there is no express provision of 'addition' of facilities or the approving officer or his ranking in the Ordinance. Nor is there any definition of the scope or extent of facilities that can be added in this manner. For instance, it is not clear whether the departmental approving officer could approve the addition of a facility that has previously been refused or revoked by a panel judge. I have advised the LEAs that in such circumstances, they should seek the approval of the panel judge to intercept the additional facility instead of having it approved within the department.

13.9 During my inspection visit to one of the LEAs, I noted a case where the original authorization granted by a panel judge contained the 'reasonably expected to use' clause but the renewed authorization did not. The LEA took it that since the original authorization contained such wording and the same was asked for in the application for renewal, the renewed authorization should also empower it to add facility(ies)

reasonably expected to be used by the targeted subject even though this was not expressly stated in the renewed authorization. I clarified this with the panel judges and they unanimously disagreed. The fact that an original authorization for interception contained the 'reasonably expected to use' wording does not necessarily mean that the same latitude would be granted in the renewed authorization unless such wording is expressly stated in the renewed authorization by the panel judge. I advised the LEA concerned that its interpretation of the panel judge's renewed authorization was wrong and the LEA confirmed that it had not added any facility under the renewed authorization.

13.10 Initially, the LEAs did not feel the need to report to the panel judges as to the facilities which they had added by virtue of the 'reasonably expected to use' clause in a prescribed authorization, apparently because there is no such reporting requirement stipulated in the Ordinance or the Code of Practice. On my recommendation, the LEAs agreed to report such addition of facilities to the panel judges by treating the addition as a material change of circumstances that ought to be brought to the attention of the panel judges as one of the conditions upon which their authorizations were granted.

13.11 To avoid any ambiguity in the legality of facilities added by LEAs themselves, I **recommend** that the Ordinance should have an express provision on this, including the definition of the ambit of facilities that can be added in this manner and the requirement to report to the panel judge as soon as reasonably practicable after the departmental approving officer has exercised his power to intercept additional facilities that the subject is reasonably expected to use.

(3) Imposing conditions when confirming emergency authorization

13.12 The Security Bureau holds the view that under the statutory scheme, a panel judge cannot impose additional conditions when confirming an emergency authorization. If a panel judge wishes to do so, he would need to first refuse the application and then make a separate order under section 24(3)(a) of the Ordinance.

13.13 However, the panel judges do not agree that a panel judge cannot impose any additional conditions when confirming an emergency authorization. They refer to the provision in section 32 of the Ordinance which provides that –

> 'A prescribed authorization may be issued or renewed **subject to any conditions** specified in it that apply to the prescribed authorization itself or to any further authorization or requirement under it …' (Emphasis added.)

They consider that section 24 cannot be used in isolation since the definition of 'prescribed authorization' includes an emergency authorization.

13.14 The conflicting interpretations held by the Security Bureau and the panel judges may be addressed when the Ordinance is next revised.

(4) Revocation of device retrieval warrant

13.15 Where a prescribed authorization has ceased to have effect, an officer of the department may apply to a panel judge under section 33 of the Ordinance for the issue of a device retrieval warrant authorizing the retrieval of any of the devices authorized to be used under the prescribed authorization if such devices have been installed in or on any premises or object pursuant to the prescribed authorization and are still in or on such premises or object, or are in or on any other premises or object. A device

retrieval warrant takes effect at the time specified by the panel judge and ceases to have effect upon the expiration of the period specified by the panel judge which in any case is not to be longer than a period of three months.

13.16 One can find in section 57 of the Ordinance express provision for the revocation of the prescribed authorization by the relevant authority after receiving a report on discontinuance of the authorized interception or surveillance. However, there is no similar provision in the Ordinance with regard to the revocation of a device retrieval warrant. I have recommended to the Secretary for Security that although there is no statutory provision, in case a device retrieval warrant is discontinued, say, because the relevant purpose has been achieved or it has become unable to retrieve the device specified in the warrant, there is a need to report the discontinuance to the panel judge for him to revoke the device retrieval warrant.

13.17 The Security Bureau's response is that the reason for not providing for revocation of device retrieval warrants in the statutory scheme (as compared to prescribed authorizations) is that device retrieval warrants authorize the carrying out of specified tasks. When a device is successfully retrieved, the task is completed. There is no more device to be retrieved and the need to revoke the warrant does not arise as the warrant does not give authority for any other actions. On the other hand, a failed attempt to retrieve a device would not result in the warrant ceasing to have effect. The LEA concerned could make further attempts to retrieve the device within the validity period of the warrant in question. The warrant ceases to have effect at the end of the validity period specified if the device has not by then been retrieved.

13.18 According to the Security Bureau's understanding, there is no legal authority for a panel judge to revoke a device retrieval warrant, since the warrant is a statutory creation, and there is no statutory power under the Ordinance (nor under the Interpretation and General Clauses Ordinance (Cap 1)) which would permit its revocation.

13.19 The panel judges, however, share my view and reckon that although there is no statutory provision, there is still a need for panel judges to revoke the warrant in cases, for example, where the address is found to be incorrect after the granting of the warrant.

13.20 I **recommend** that there should be an express provision in the statute to require the LEAs to report to the panel judges the discontinuance of device retrieval warrants and for the judges to revoke device retrieval warrants where necessary.

(5) Commissioner's power under section 53

13.21 Section 53(2) empowers me to request a panel judge to provide me with access to any of the documents or records kept under section 3 of Schedule 2 for the purpose of performing any of my functions under the Ordinance.

13.22 In the performance of my duty to oversee the compliance by LEAs, I made a request to the panel judges for providing me, on a weekly basis, with copies of certain types of documents kept under section 3 of Schedule 2 as and when they are used so as to enable me to counter check the information in the weekly reports submitted by LEAs to me. The essential information relating to the identifying details of the targeted subject should be blocked out from the copy documents so that the risk of security leakage would be reduced to the minimum, if not entirely

eliminated. Previously the counter checking was done by my requesting the panel judges to complete weekly report forms identical to those requested from the LEAs, but the panel judges were perturbed at the large amount of details to be provided in the weekly report forms. My request to the panel judges for copy documents was an alternative adopted to reduce their efforts or facilitate their work.

13.23 While the panel judges welcome the convenience of my proposed alternative they have, however, grave doubts on whether they can provide me with the copy documents as requested. They refer to the following provisions in Schedule 2 that prescribe how all documents and records compiled by, or made available to, the panel judges are to be handled by them:

(a) Section 3(1) thereof provides that these documents are –

> '… to be kept in a packet sealed … as soon as they are no longer immediately required for the purpose of performing any of [the panel judges'] functions …'.

(b) Section 3(2) thereof stipulates (among other things) that the panel judge to whom these documents are made available shall –

> '… cause … [a certified] copy [of each of those documents] … to be made available to the department concerned'.

13.24 The panel judges also point out that under section 53(2) of the Ordinance, the Commissioner may request the panel judges to provide him with **access to** those documents. The Chinese version of section 53(2) reads –

> '專員可…向小組法官要求讓他可取用[該等文件]'.

13.25 However, in view of the absence of express provision for their doing so, the panel judges have grave doubts on whether the Ordinance permits them to provide any copy of the documents to the Commissioner in addition to making available copies to 'the department concerned'.

13.26 The panel judges' view is supported by a written legal advice from the Department of Justice. While the adviser accepts that section 53(2) may impliedly empower the panel judges to provide copies of the documents to the Commissioner, he is of the opinion that routinely copying the documents is not envisaged by the Ordinance and cannot be justified by the Commissioner's general oversight function for which the copy documents are requested.

13.27 I cannot agree with these interpretations. Section 53(2) permits me to have access to and even take away (取用) any of the documents or records kept by the panel judges under section 3 of Schedule 2 for the performance of my functions under the Ordinance. The bigger includes the lesser. If I am permitted to take away even the original documents, it would be absurd if the law were not to allow the panel judges to make a photocopy for me in the due performance of my functions. Even if a much more restrictive construction of 'access' is adopted, I would be entitled to have the documents made available to me, view them, take written notes of them and hand-copy them, but on the said interpretations I would not be allowed to have a photocopy of them. In such a case, whenever I wish to view any of the documents for obtaining any information contained in them, I would have to personally visit the PJO and read the documents, and I would have to hand-copy them if I wish to keep a record of what I have read. Since the documents are packaged under seal and stored in a secure room in the PJO, a panel judge would have to return

to the PJO to break the seal and accompany me for my viewing and physically copying the documents. The personal service of a panel judge and mine in this regard could not be dispensed with or replaced by deploying an officer from our respective offices for the purpose.

13.28 The legal advice suggested that my power to request copy documents from the panel judges should be restricted to specific cases where discrepancies (whatever those might be, between the information provided to me by the LEAs and the PJO) have arisen instead of in the routine performance of my oversight function cannot be justified. Unless the PJO's weekly return contains identical details as those contained in the LEAs' weekly returns, there will be no basis for comparison to be made to expose any discrepancy to give rise to the suggested proper exercise of my power. As described in paragraph 13.22 above, the panel judges wished to avoid providing such large amount of details, and without such details or the copy documents as the alternative, my task in counter checking would be rendered ineffective, if not futile. Moreover, section 53(5) empowers me to determine the procedure to be adopted in performing any of my functions under the Ordinance, and imposing the suggested restriction pays lip service to this provision. Nor would the fear of security leakage be a warrant for such a restriction, because the essential information relating to the identifying details of the targeted subject would have been blocked out and after all the Commissioner's appointment should be safely relied on to bear out that full security measures had been taken and that he could be trusted with the secretive nature of the work.

13.29 The different views of construction held by the panel judges and the legal advice on the one hand and me on the other can be resolved by amending section 53 of the Ordinance or section 3(2) of Schedule 2 to

make express provision that a copy of documents kept under section 3 of Schedule 2 could also be made available to the Commissioner by the panel judges upon the Commissioner's request.

(6) Examination and notification by the Commissioner

13.30 There is also an absence of express provision as to what I, as the Commissioner, should do when discovering that there was an unauthorized statutory activity, when an application for examination has been received. According to section 44(2), when in dealing with such an application I determine that there has been an unauthorized statutory activity, I shall notify the applicant that I have found the case in his favour and initiate the procedure for assessing and awarding compensation to him [section 44(2), (3) and (4)]. Moreover, if I discover that there has been an unauthorized statutory activity during the performance of my functions under the Ordinance, I shall give notice to the affected or relevant person to advise him of his right to make an application for examination whereby the compensation procedure can also be invoked [section 48(1) and (2)]. However, according to sections 44(6) and 48(3), I will only give such notice when I consider that it would not prejudice the prevention or detection of crime or the protection of public security. In practice, if the unauthorized activity is discovered by me, without anyone applying for examination, I can rely on section 48(3) to refrain from giving the notice to the affected person, because he would not know my discovery. However, if the affected person makes an application for examination pursuant to section 43 without having been prompted by my notice under section 48(1), then according to section 44(2), I am obliged to give him the notice if my doing so would not prejudice the prevention or detection of crime or the protection of public security. If I consider that section 44(6) is applicable

in that such prejudice would be caused by giving the notice, what am I to do if I, as allowed by section 44(6), do not give the applicant the notice? The notice that I do not find the case in his favour referred to in section 44(5) does not seem to be suitable because the content of such a notice does not adhere to the fact that I have determined that there was an unauthorized statutory activity carried out against him, based on which fact section 44(2) would require me to give a notice of a finding in his favour. Moreover, a notice not favouring the applicant's case under section 44(5) might be accused of containing a lie. The wording of section 44(6) excepting the Commissioner from giving a notice notwithstanding the provisions of subsections (2), (3) and (5) is not wide enough, in my view, to authorize me to give a notice under subsection (5). If no notice is given to the applicant under either section 44(2) or under section 44(5), especially after a few months, he would appreciate that he was or still is a subject of one or more statutory activities, albeit unauthorized and would accordingly take avoidance action. This situation is, ironically, what section 44(6) is apparently aimed to prevent.

13.31 To cater for the situation mentioned above, I **recommend** that amendments be made to section 44(6) and section 48(3) to provide the Commissioner with the legal basis for giving a notice in terms of that in section 44(5).

13.32 Section 45(1) gives discretion to and section 45(2) imposes an obligation on the Commissioner not to carry out the examination applied for by an applicant for examination. However, there is no provision as to what the Commissioner should do in response to the applicant's application where a situation covered by either of the subsections of section 45 arises. If the Commissioner notifies the applicant that he is not proceeding with

the examination, would he not be required to give a reason for his so refraining? Even if the Commissioner is exempt from giving a reason, the applicant would without any difficulty appreciate that his case was not that covered by any of the situations under section 45(1), ie, that his application was made more than 1 year after the statutory activity complained of took place, that the application was made anonymously, that the applicant cannot be identified or traced or that the application is frivolous or vexatious or not made in good faith, and therefore he would be able to come to the conclusion that his case was that under section 45(2), ie, relevant criminal proceedings are pending or are likely to be instituted. Or alternatively, since he has received no notice from the Commissioner, he might think that his case falls within the situation covered by section 44(6) with the consequence already referred to in paragraph 13.30 above. In either event, the applicant's appreciation of the reason(s) for not receiving a response from the Commissioner would undoubtedly be compromising the prevention or detection of crime or the protection of public security.

13.33 To cater for the situation mentioned in the preceding paragraph, I **recommend** that section 45 be amended to add a provision giving the Commissioner the legal basis for giving a notice in terms of that in section 44(5) even where he is not going to proceed with the examination sought by the applicant.

(7) Practical difficulty regarding the application of section 58

13.34 Section 58(1) provides that where the officer of the department concerned who is in charge of the statutory activity becomes aware that the subject of the statutory activity has been arrested, the officer shall as soon as reasonably practicable cause to be provided to the relevant

authority a report assessing the effect of the arrest on the likelihood that any information which may be subject to LPP will be obtained by continuing the statutory activity. Where the relevant authority receives a report under subsection (1), he shall revoke the prescribed authorization if he considers that the conditions for the continuance of the prescribed authorization under section 3 are not met, and the prescribed authorization is to cease to have effect from the time of the revocation [subsections (2) and (3)].

13.35 The report on arrest under section 58 is to be distinguished from the situation of a report on discontinuance under section 57. The discussion on the topic is contained in paragraphs 11.20 to 11.22 of Chapter 11. Where a report of arrest under section 58 is made, the LEA officer making the report obviously wishes the relevant authority to continue the validity of the prescribed authorization despite the arrest of the targeted subject, or else he would have already discontinued the authorized activity and reported on the discontinuance under section 57. No problem will arise if the relevant authority receiving the section 58 arrest report decides not to revoke the authorization, but there will be practical difficulties if the decision is otherwise.

13.36 It was during an inspection visit to an LEA towards the end of March 2007 when enquiries were made of its officers as to each and every of the steps taken where situations under section 57 and section 58 arose that it dawned on the Commissioner that an irregularity might arise from the application of the section 58 procedure.

13.37 Where the relevant authority to whom a section 58 arrest report is made decides to revoke the prescribed authorization, there would

be an interim period during which the interception or surveillance would remain in operation after the prescribed authorization (which is sought to be continued) is revoked but before the revocation (with immediate effect) is conveyed to officers carrying out the operation. The interception or surveillance carried out during the interim period would in the circumstances become in theory an unauthorized activity.

13.38 The LEAs were advised of the possible irregularity and required to report on the cases in which such irregularity had taken place. Since the commencement of the Ordinance on 9 August 2006 and up to the end of March 2007, there were four cases of interception falling within the situation described in the preceding paragraph, two of which occurred during the report period.

13.39 I have discussed with the panel judges and we are all agreed that section 58 in its present wording does not allow the panel judges to post-time the revocation.

13.40 One way of addressing the problem is to discontinue the statutory activity temporarily at the time of submitting the arrest report to the relevant authority and re-start the activity if the relevant authority decides not to revoke the prescribed authorization. But this has the undesirable effect of missing the intelligence in between and is not conducive to the prevention or detection of crime or the protection of public security in the event that the relevant authority does not revoke the prescribed authorization after considering the report of arrest.

13.41 The same problem would arise if an emergency authorization when being revoked in accordance with section 24(4) is still in operation. It equally applies to a revocation under section 27(3)(a)(i) and (4) of an

authorization issued upon oral application. Fortunately, no such case has yet occurred.

13.42 The Security Bureau has recently prepared a paper on the subject. It points out that the same problem also applies to the scenario where consequent upon an LEA's report to the PJO of a material change of circumstances regarding a prescribed authorization granted by a panel judge, the panel judge writes on the report that the prescribed authorization is revoked.

13.43 While it appears to me that a solution would be to amend the relevant provisions of the Ordinance to allow the relevant authority flexibility to defer the time of revocation of prescribed authorizations to some time as the relevant authority will state in the revocation, the Security Bureau paper has suggested pragmatic ways, which have to be adopted by the panel judges, to resolve the difficulties for the consideration by the panel judges and me. No decision on the suggested ways has yet been made pending the completion of this report.

13.44 In the meantime, I have advised the LEAs to follow the arrangement referred to in paragraph 13.40 above to avoid any possible unauthorized interception or surveillance caused by the revocations of the authorizations discussed under this section.

(8) Separate listing required by section 49(2)

13.45 Section 49(2) of the Ordinance provides that the Commissioner's annual report to the Chief Executive is to set out various matters 'separately in relation to interception and covert surveillance'. Such matters are to be contained in lists referred to in paragraphs (a), (b), (c)

and (d) of the subsection and to include an assessment on the overall compliance under the remaining paragraph (e) of the subsection.

13.46 While the matters to be shown in the lists under section 49(2)(a) can be readily appreciated as required to be separately listed to distinguish between 'interception' and 'covert surveillance', I find it difficult to understand the identical requirement regarding 'the major categories of offences' under paragraph (b)(i), 'the number of persons arrested' under paragraph (b)(ii), matters under paragraph (c), 'a summary of reviews conducted by the Commissioner under section 41' under paragraph (d)(i), other matters under paragraph (d), and 'an assessment on the overall compliance with the relevant requirements' under paragraph (e). It seems to me that the umbrella heading of 'separately in relation to interception and covert surveillance' in the lead-in wording of section 49(2) does not make too much sense when applied to the matters under paragraphs (b), (c), (d) and (e) of that subsection and should better be left out. Indeed, requiring a distinction to be made on such matters may prejudice the prevention or detection of crime or the protection of public security; for example, the categorization of offences with the distinction may help criminal minds to evaluate what kind of investigation activity would more likely be employed by LEAs for a particular kind of offence.

13.47 I **recommend** that this matter be looked into when the Ordinance is next revised.

CHAPTER 14

CONCLUSIONS AND ACKNOWLEDGEMENT

14.1 I have reviewed the compliance by the LEAs with the requirements of the Ordinance in Chapter 4. Overall, I find it satisfactory. Please see the discussions in paragraphs 4.11 to 4.20 under the heading 'Review of compliance'.

14.2 During the report period, I did not detect any deliberate breach of the requirements of the Ordinance or the Code of Practice by any LEAs or their officers. The irregularities reported in Chapter 10 were genuine careless mistakes and the heads of LEAs have taken appropriate follow up actions to prevent recurrence. The unauthorized statutory activities stated in paragraph 13.38 of Chapter 13 were caused by the non-realisation of the irregularity given rise by the practical difficulty in discontinuing the statutory activities at the same time as the revocation of the authorization and were not intentional.

14.3 In Chapter 9 and Chapter 11, I have outlined the recommendations I made to the Secretary for Security and the LEAs respectively to better carry out the objects of the Ordinance and the Code of Practice. Most of them were accepted by the Secretary for Security and the heads of LEAs for implementation.

14.4 In the light of my experience obtained after the operation of the Ordinance for some months and of the different or even conflicting interpretations of the provisions of the Ordinance adopted by the panel judges, the Security Bureau, the LEAs and myself, I have in Chapter 13 of this Report reviewed certain provisions of the Ordinance and made

consequential recommendations. A summary of these recommendations is given below:

(a) To amend section 57 of the Ordinance to indicate whether a panel judge has the power to partially revoke an authorization [paragraphs 13.5 to 13.7].

(b) To expressly provide in the Ordinance to make clear the extent of the LEAs' power to include in the prescribed authorization for interception of telecommunications services that a subject is reasonably expected to use, to define the ambit of such telecommunications services that can be so added, and to require the LEAs to report to the panel judges after exercising such power [paragraphs 13.8 to 13.11].

(c) To spell out in the Ordinance whether a panel judge has the power to impose additional conditions when confirming an emergency authorization [paragraphs 13.12 to 13.14].

(d) To make express provision in the Ordinance to require LEAs to report to the panel judges the discontinuance of device retrieval warrants and for the panel judges to revoke device retrieval warrants where necessary [paragraphs 13.15 to 13.20].

(e) To amend section 53 of the Ordinance or section 3(2) of Schedule 2 to provide expressly that a copy of the documents kept under section 3 of Schedule 2 could also be made available to the Commissioner by the panel judges upon the Commissioner's request [paragraphs 13.21 to 13.29].

(f) To amend sections 44(6), 45 and 48(3), and related provisions, to provide the Commissioner with the legal basis for giving a

notice (to the applicant for examination under section 43 or the relevant person under section 48) in terms of that in section 44(5) [paragraphs 13.30 to 13.33].

(g) To amend section 58 and also sections 24 and 27 to allow the relevant authority flexibility to defer the time of revocation of the prescribed authorization to some time as the relevant authority will state in the revocation, unless the pragmatic ways suggested by the Security Bureau are accepted [paragraphs 13.34 to 13.44].

(h) To re-consider the requirement to list separately in relation to interception and surveillance matters referred to in paragraphs (b) to (e) of section 49(2) regarding the Commissioner's annual report to the Chief Executive [paragraphs 13.45 to 13.47].

14.5 When the occasion to revise the provisions of the Ordinance arises, consideration should also be given to the amendment of its name and the Commissioner's title [paragraph 1.5 of Chapter 1].

14.6 I am grateful to the PJO, the Security Bureau, the LEAs, the CSPs and other concerned parties for their cooperation and assistance in the performance of my functions to ensure full compliance with the Ordinance and the Code of Practice to protect the privacy of citizens in Hong Kong. I look forward to their continued support.