THE LAW REFORM COMMISSION OF HONG KONG

REPORT

PRIVACY : REGULATING THE INTERCEPTION OF COMMUNICATIONS

This report can be found on the Internet at:
<http://www.hkreform.gov.hk>

December 1996

The Law Reform Commission was established by His Excellency the Governor in Council in January 1980. The Commission considers such reforms of the laws of Hong Kong as may be referred to it by the Attorney General or the Chief Justice.

The members of the Commission at present are:

The Hon Mr J F Mathews, CMG, JP
(Attorney General) (Chairman)
Mr Tony Yen (Law Draftsman)
The Hon Mr Justice J Chan
Mr Eric Cheung
Professor Yash Ghai, CBE
Professor Kuan Hsin-chi
Dr Lawrence Lai
Mr Andrew Liao, QC
Mr Gage McAfee
Mr Alasdair G Morrison
Mr Robert Ribeiro, QC
Professor Derek Roebuck
Professor Peter Wesley-Smith
Mr Justein Wong Chun, JP

The Secretary of the Commission is **Mr Stuart M I Stoker** and its offices are at:

20/F Harcourt House,
39 Gloucester Road,
Wanchai,
Hong Kong.

Telephone: 2528 0472
Fax: 2865 2902
E-mail: hklrc@hkreform.gov.hk

A summary of this report, and other information on the Commission, can be found on the Internet at:<***http://www.hkreform.gov.hk***>

Mr Godfrey K F Kan*, Crown Counsel, was principally responsible for the writing of this Commission report.*

THE LAW REFORM COMMISSION OF HONG KONG

REPORT

PRIVACY: REGULATING THE INTERCEPTION OF COMMUNICATIONS

CONTENTS

Introduction

Terms of Reference

1. On 11 October 1989, under powers granted by the Governor-in-Council on 15 January 1980, the Attorney General and the Chief Justice referred to the Law Reform Commission for consideration the subject of "privacy". The Commission's terms of reference are as follows:

> *"To examine existing Hong Kong laws affecting privacy and to report on whether legislative or other measures are required to provide protection against, and to provide remedies in respect of, undue interference with the privacy of the individual with particular reference to the following matters:*
>
> *(a) the acquisition, collection, recording and storage of information and opinions pertaining to individuals by any persons or bodies, including Government departments, public bodies, persons or corporations;*
>
> *(b) the disclosure or communication of the information or opinions referred to in paragraph (a) to any person or body including any Government department, public body, person or corporation in or out of Hong Kong;*
>
> *(c) intrusion (by electronic or other means) into private premises; and*
>
> *(d) the interception of communications, whether oral or recorded;*
>
> *but excluding inquiries on matters falling within the Terms of Reference of the Law Reform Commission on either Arrest or Breach of Confidence."*

2. The Law Reform Commission appointed a sub-committee to examine the current state of legislation and to make recommendations ("the sub-committee"). The members of the sub-committee are:

The Hon Mr Justice Mortimer (Chairman)	Justice of Appeal
Dr John Bacon-Shone	Director, Social Sciences Research Centre, The University of Hong Kong

Mr Don Brech	Principal Consultant Records Management International Limited
Mrs Patricia Chu	Deputy Director (Services) Social Welfare Department
Mr A F M Conway	Chairman Great River Corporation Limited
Mr Edwin Lau	Assistant General Manager (Retail Banking) Hongkong & Shanghai Banking Corporation
Mr James O'Neil	Deputy Crown Solicitor Attorney General's Chambers
Mr Peter So Lai-yin	General Manager Hong Kong Note Printing Limited
Prof Raymond Wacks	Professor of Law and Legal Theory The University of Hong Kong
Mr Wong Kwok-wah	Bureau Chief Asia Times

3. The Secretary to the sub-committee was initially Mr Mark Berthold, Consultant. He was succeeded by Mr Godfrey Kan, Crown Counsel, in March 1996.

4. The issues raised at items (a) and (b) in the terms of reference were addressed in the Law Reform Commission report on *Reform of the Law relating to the Protection of Personal Data* published in August 1994. Most of the recommendations of that report were adopted with the enactment of the Personal Data (Privacy) Ordinance (Cap. 486) on 3 August 1995. This report deals mainly with item (d).

Surveillance and interception of communications

5. Although this report mainly deals with the interception of communications, both intrusion into private premises and the interception of communications impinge on an individual's right to privacy. An attempt is therefore made in this introduction to explore the relevant privacy concerns. This is followed by an explanation of how the new surveillance technologies affect an individual's privacy.

6. It should be made clear at the outset that the references to "intrusion (by electronic or other means) into private premises" and "the interception of communications" in the terms of reference are not separate; they overlap in some situations. For example, it is now possible to "read" electronic mail by monitoring the radiation emitted by a word processor by

remote means. This could fall under either (c) or (d) in the terms of reference. Similarly, the use of a listening device planted in a telephone handset or speaker phone is covered by both (c) and (d); the planting of the listening device necessitates an intrusion into private premises and the use of the device facilitates the interception of communications transmitted by telephone lines.

7. Although this report makes frequent reference to new technologies affecting privacy, a regime which regulates surveillance activities should not focus on such technologies. Regulation must be founded on general principles. Nonetheless, an awareness of new applications of technology provides a means of checking that any proposed regulatory framework effectively covers the various means of intrusion.

Relationship with data protection

8. In our consideration of the first part of the reference, we examined the protection of personal data. The principal focus of data protection is the regulation of data relating to the individual, whether the data are collected from the individual or from a third party. When data are collected or acquired, they become subject to the application of the data protection principles. The regulation of intrusion upon privacy focuses on protecting the individual at the stage when information is acquired about him, whether or not it is captured as recorded data.

9. Insofar as most surveillance and interception of communications will be conducted with the specific purpose of collecting data records, a data protection regime represents a significant source of control. Nonetheless, as Wacks points out, although of practical significance, the collection of personal data is not the primary concern arising from the use of surveillance techniques, but rather that the surveillance process itself constitutes an interference with the privacy of the individual:

> *"My objection to being watched or to having my telephone tapped is not necessarily that 'personal information' about me has been obtained, for the activities that are observed or the conversations that are monitored do not necessarily involve 'personal information'. Certainly, it is the main purpose of the intruder to obtain information about an individual, and some of the information may well be 'personal' ... . But it should be stressed that there is no necessary connection between the acquisition of 'personal information' and the individual's interest in not being observed ... . When my telephone is tapped my principal objection is that there has been an intentional interference with my interest in seclusion or solitude."*[1]

[1] Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989) at 248-9.

The relevance of privacy today

10. A number of developments in recent years have increased public awareness of privacy issues and the threats posed to privacy in daily life:

(a) The enactment of the Personal Data (Privacy) Ordinance (Cap. 486) in 1995 has brought privacy issues to the fore. Enforcement of the provisions of the Ordinance is likely to heighten awareness of the importance of protecting privacy and personal information.

(b) The rapid expansion of the Internet, and the resultant increase in the amount of personal information available on-line, has made the public more concerned about the privacy of their communications. Service companies are likely to use privacy as a competitive weapon in winning customers.[2]

(c) The growth in the use of electronic communications systems by industry has increased the need for security of those communications in such areas as banking and finance. Service carriers are aware that an inability to safeguard customer information will adversely affect customer relations and their business. Another concern is that of theft of proprietary information.

(d) The development of advanced communications networks is likely to be hindered unless service carriers can assure the public that there is adequate security for their communications. The President of the United States Telephone Association asserts that:

> *"If the public becomes skittish about using the public network for fear either that it is full of 'back doors' designed so that their local sheriff will be developing a dossier on them based on call set-up information, that fear will translate into reduced use of the system. The result will be the loss of billions of dollars in potential revenue, and along with that many of the jobs, the taxes, and the benefits that we anticipate from the information age."*[3]

Interception of telecommunications and data protection

11. The Australian Telecommunications Authority points out that the telecommunications industry has specific characteristics which include a global nature, high infrastructure costs, and rapidly developing technologies.

---

2 H J Smith, *Managing Privacy: Information Technology and Corporate America* (1994).

3 *Prepared Testimony of Roy Neel before the Senate Judiciary Subcommittee on Technology and the Law*, 18 March 1994, collected in David Banisar (ed), Electronic Privacy Information Centre ("EPIC"), *1994 Cryptography and Privacy Sourcebook* (Diane Publishing, Upland, Pennsylvania, 1994), Part III.

It observes that "using telecommunications means for conveying personal information does not by itself comprise an issue of telecommunications privacy".[4] It recommends that measures to control the collection and use of personal data by means of telecommunications networks should accord with the data protection principles.

12. The Ontario Information and Privacy Commissioner usefully distinguishes three types of personal information collected and processed by telecommunications carriers or service providers:

- data obtained at the time of application to be connected to the network, including name and address for service and billing (customer information);

- data captured at the time a call is made, including number called and duration of call (transactional or billing information); and

- the content of the communication itself (the conversation or message).

13. The Commissioner argues that subscribers understand that customer and billing data will need to be collected by the service providers as an adjunct to the service. He points out, however, that subscribers would not regard it as reasonable for the content of the conversation or message to be subject to collection.

14. In the Hong Kong context, upon collection, those data will be subject to the application of the data protection principles pursuant to the Personal Data (Privacy) Ordinance (Cap. 486).[5] Our task in this part of the reference is to consider protection against serious intrusions which supplements the more general provisions of the Ordinance.

Corporate privacy and individual privacy

15. Although we mentioned that our task can be seen as supplementing the provisions of the Personal Data (Privacy) Ordinance, our scope of enquiry is wider than the scope of the Ordinance. Our study will cover all types of surveillance and interception of communications whether the communications or activities in question involve personal data or commercial data. The content of a communication or the nature of the activities are irrelevant to the protection of an individual's privacy. The privacy of the individual should be protected whether he is engaging in business or

---

[4] Australian Telecommunications Authority (AUSTEL), *Telecommunications Privacy* (Melbourne, 1992), paragraph 3.48 *et seq.*

[5] In particular data protection principle 3 which provides that personal data shall not, without the consent of the data subject, be used for any purpose other than the purpose for which the data were to be used at the time of the collection. See section 4 and schedule 1 to the Ordinance.

private affairs. Both business and personal communications should therefore be protected.

16. We are aware that commercial or personal data may be communicated between machines, with no human intervention. These communications should also be regulated because the machines are merely used as a medium to send and receive communications on behalf of two individuals. An example is where a message is recorded and stored for subsequent transmission between voice mail machines.

The interests requiring protection from intrusion

17. As was pointed out in our report on the protection of personal data, a key word in the terms of reference is "privacy". In his comprehensive review, Wacks concludes that "in spite of the huge literature on the subject, a satisfactory definition of 'privacy' remains as elusive as ever."[6] We set out in the following paragraphs some of the more influential definitions of "privacy."

18. The Justice Report defined "privacy" as meaning:

> *"that area of a man's life which, in any given circumstances, a reasonable man with an understanding of the legitimate needs of the community would think it wrong to invade."*[7]

19. Westin argues that privacy is:

> *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve."*[8]

20. The Calcutt Committee defined it as:

> *"The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information."*[9]

21. While the Younger Committee concluded that the concept of privacy could not be satisfactorily defined, it identified two principal privacy interests:

---

6 Wacks, *op cit*, at 13.
7 JUSTICE, *Privacy and the Law* (1970), para 19.
8 A F Westin, *Privacy and Freedom* (1967), p 7.
9 *Report of the Committee on Privacy and Related Matter*, (Cmnd 1102, 1990).

"The first of these is freedom from intrusion upon oneself, one's home, family and relationships. The second is privacy of information, that is the right to determine for oneself how and to what extent information about oneself is communicated to others."[10]

22. The Australian Law Reform Commission follows the approach suggested by McCloskey:[11]

"Privacy is an ordinary language word, an ordinary language concept, not a finely honed philosophical or legal concept. This means that we may well find incoherences, inconsistencies in the ordinary concept such that, to be made clear, coherent, useful concept, it needs to clarified, modified, and made to be such. However, if this is done in a very radical way, the new concept may lose its relevance to the ordinary language concept. I suggest therefore that the concept be explicated as closely as possible to the ordinary usage concept, and then, if privacy so understood seems in certain respects not to merit, or not to lend itself to, legal protection and assistance, this be said."

23. According to this approach, the first step is to ascertain the ordinary language meaning and thereafter determine whether the "privacy interests" so encompassed should, as a matter of policy, be protected. Relevant factors to this latter inquiry include the requirements of the International Covenant on Civil and Political Rights, the Hong Kong Bill of Rights Ordinance (Cap. 383) and the Basic Law.

Article 17 of the ICCPR

24. Article 17 of the International Covenant on Civil and Political Rights ("the ICCPR") is replicated as article 14 of the Hong Kong Bill of Rights (Cap. 383, Part II). It provides:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks. "

25. The United Nations Human Rights Committee makes the following comments on this article:

---

10 *Report of the Committee on Privacy ("the Younger Report")*, (Cmnd 5012, 1972), para 38.

11 See Australian Law Reform Commission, *Privacy* (Report No 22, 1983), vol 1, chapter 1; H J McCloskey, "*Privacy and the Right to Privacy*", (1980) 55 *Philosophy Quarterly* 17.

- This right must be guaranteed against all arbitrary or unlawful interferences and attacks, whether they emanate from State authorities or natural or legal persons.

- The primary method of providing such protection is state legislation. No interference may take place except in cases envisaged by the law.

- The inclusion of the expression "arbitrary interference" is "intended to guarantee that even interference provided for by law should accord with the Covenant and should be, in any event, reasonable in the particular circumstances."[12]

26. Regarding the contents of such legislation as it relates to surveillance and interception, the Human Rights Committee states:

> *"Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis. Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited ... . States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons."*[13]

27. The jurisprudence interpreting the similarly worded privacy provision of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("the European Convention") is also relevant to the interpretation of article 17 of the ICCPR. Article 8 of the Convention provides:

> *"1. Everyone has the right to respect for his private and family life, his home and correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in*

---

12 Cf *Ex parte Lee Kwok-hung* [1993] 2 HKLR 51, at 63.

13 General Comment 16/32 of 23 March 1988, paras 8 and 9, reproduced in M Nowak, *U. N. Covenant on Civil and Political Rights: CCPR Commentary* (1993) at 865.

the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

28. The first limb of article 8 is in virtually identical terms to article 17 of the ICCPR, and both are derived from the privacy provision of the Universal Declaration of Human Rights. However, unlike the ICCPR provision, article 8 of the European Convention imposes an explicit obligation. Article 17 of the ICCPR instead focuses on protection from interference, but this presupposes an affirmative right to respect for privacy.

29. Article 17 specifically provides protection for family, home, and correspondence. These expressions are reasonably clear and apply to surveillance of domestic premises. The European Court held in *Klass*[14] that "correspondence" encompasses all telecommunications. In ascertaining the scope of protection from surveillance in other spheres, recourse must be had to the word "privacy". In contrast to article 17, article 8 of the European Convention refers to "private life" rather than "privacy", but nothing turns on this. *Klass* ruled that telephone tapping not only constitutes an interference with the individual's "correspondence" but also with his private life. As regards other methods of spying, the only case apparently reported on this aspect of article 17 dealt with surveillance of the applicant's youthful participation in political activities.[15] In her analysis, Doswald-Beck concludes that the ruling of the European Commission of Human Rights in that case appears to be premised on the assumption that secret surveillance of an individual other than by telephone tapping "may well amount to an interference with private life".

30. It is also arguable that the principles laid down in *Klass* are not restricted to telephone tapping, although that form of surveillance is specifically dealt with. Certainly the language of the Court often speaks of "surveillance" generally, rather than the specific technique in question.

The Basic Law of the Hong Kong Special Administrative Region

31. As from 1 July 1997, the system for safeguarding the fundamental rights and freedom of Hong Kong residents will be based on the provisions of the Basic Law of the Hong Kong Special Administrative Region.[16] The following provisions in the Basic Law indicate that arbitrary or unlawful intrusion into private premises will continue to be prohibited and that the privacy of communications may not be infringed except to meet the needs of public security or investigation of crime:

---

14 *Klass v Federal Republic of Germany* (1978) 2 EHRR 214.

15 Application No *8170/78, X v Austria*.

16 Basic Law, article 11.

*"**Article 29** The homes and other premises of Hong Kong residents shall be inviolable. Arbitrary or unlawful search of, or intrusion into, a resident's home or other premises shall be prohibited."*

*"**Article 30** The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."*

32. The Basic Law also guarantees that the provisions of the ICCPR will remain in force after the handover and will be implemented through the laws of Hong Kong. Any restriction imposed by the laws on the rights and freedoms of Hong Kong residents must be consistent with the provisions of the ICCPR.[17]

Modern surveillance technology

33. To understand the scope and nature of the problem posed by intrusions on privacy, it is necessary to have some knowledge of the surveillance technology which is now available.

34. The development of new surveillance technology has had a significant impact on the ability of the individual to protect his privacy. Cameras are now capable of taking photographs in the dark; conversations inside a room can be recorded by applying laser beams to the window from the outside; and information stored in a computer can be read off a video display unit by the implantation of a listening device, a remotely operated camera, or the re-creation of the data from electromagnetic radiation emitted by the computer.[18]

Counter-surveillance

35. The development of surveillance technology has also generated a small industry devoted to counter-surveillance. The techniques used may include:[19]

- Technical sweeps to detect such indicators as electronic pulses, surges, and radio frequencies. For example, a device is

---

17 Article 39.

18 G Marx, *Undercover: Police Surveillance in America* (London: University of California Press, 1988), at 207 and 231. M Wasik, *Crime and the Computer* (Oxford: Clarendon Press: 1991), at 52-53.

19 S Brown and G G Scott, *Private Eyes: What Private Investigators Really Do* (Citadel Press, 1991).

available to detect tape recorders, by detecting the erase oscillator on the head that erases the tape when it is recording. The oscillator signal radiates an electronic bias for several feet.

- Physical examinations.

- Active countermeasures, such as deploying jamming equipment. For example, an ultrasonic device will generate a high frequency tone above the range of normal hearing. Any attempt to record a conversation within the vicinity of the device will result only in an indecipherable high pitched sound. Another measure is the use of scramblers to render into code telephone conversations.

Use of surveillance devices in Hong Kong

36. In Hong Kong, the control and licensing of surveillance equipment is governed by the Telecommunication Ordinance (Cap. 106). Enforcement is the responsibility, not of the police, but of the Office of the Telecommunications Authority ("OFTA"). OFTA reported that there were 53 convictions for unauthorised dealing in radio equipment and 302 convictions for illegal use of amateur transceivers in 1995-96. According to a recent newspaper report[20], there is every indication that surveillance is widespread in the territory. An estimated 50 shops in Tsim Sha Tsui and Central alone sell surveillance equipment, such as a "pocket calculator" costing $8,900 which can transmit a conversation a kilometre away.

The social dimension of surveillance

37. Lustgarten and Leigh refer to the social concerns raised by the increase in electronic surveillance:

> *"One of the defining characteristics of a free person is the ability to control information about oneself. This may be important at an instrumental level: if I cannot conceal my peculiar sexual tastes, I may become unpopular, find doors to employment closed to me, or suffer some other disadvantage. More fundamental, however, is the sense of mental and emotional security that this control entails. ... If I have no control over what is known about me, I am seriously diminished as a person both in my own eyes and in those which are capable of intruding upon me. This dual aspect of respect and self-respect is a vital dimension to privacy. ...*
>
> *Clandestine interception or eavesdropping infringes upon a fundamental choice: with <u>whom</u> one chooses to speak. The*

[20] *South China Morning Post,* 21 October 1995.

only defences against it are silence and withdrawal. ... Turning inward is not merely bad for the individual personality, it is destructive of a great collective value: sociability. An atmosphere in which people practice self-censorship, avoid sharing thoughts and feelings, and prefer secretiveness for reasons of safety is stultifying and fearful."[21]

38. The undesirability of an increasing incidence of surveillance in society had been noted by the Younger Committee as long ago as 1972. The Committee observed that "in such cases, we were told, the result would be an increase in the incidence of tension-induced mental illness or at least a decrease in the imaginativeness and creativity of the society as a whole."[22]

Privacy technologies

39. While the purpose of many of the new technologies is to intrude on the individual's privacy, other technologies have been specifically developed to *protect* privacy. Some of these technologies are designed to conceal the identity of the data source. Anonymity is often the best means of securing privacy. Others, such as cryptography, scramble communication to prevent interception. However, some governments are endeavouring to restrict the individual's use of technologies designed to protect privacy. Nonetheless the development of such technologies is likely to continue and increase in importance.[23]

The relationship between surveillance techniques

40. Gary Marx classifies different types of police work according to whether they are overt/ covert or deceptive/non-deceptive.[24] He characterises most police work as *overt* and *non-deceptive,* such as the open investigation of reported crime. An example of *overt and deceptive* police work would be a uniformed officer misleading a suspect into believing that an accomplice had confessed. *Covert and non-deceptive* techniques characterise surveillance activities generally, such as hidden recording devices. But undercover work is both *covert and deceptive.* Unlike unobtrusive surveillance, undercover activities "directly intervene to shape the suspect's environment, perceptions, or behaviour". This is achieved by the use of agents posing in other roles, such as colleagues or fellow criminals.

---

21 L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994), at 39-40. See also D Lyon, *The Electronic Eye: the Rise of Surveillance Society* (Minneapolis: University of Minnesota Press, 1994).

22 Younger Report, *op cit*, at para 111.

23 We note that there is a conflict between the interests of an individual in protecting his privacy and those of the government in gaining access to telecommunications for legitimate purposes. Those who are interested in the impact of new technologies on the ability to tap into telecommunications systems, and the competing ability to encrypt messages should refer to chapter 9 of the consultation paper for further details. That chapter looks at proposals in the United States to create a government encryption standard that would facilitate the government de-scrambling encrypted voice communications.

24 *Op cit,* at 11.

Undercover activities resemble covert or deceptive tactics in that they provide a means of discovering otherwise unavailable information.

41. Marx argues that if controls are placed on one class of surveillance practices there will be a greater likelihood that other, unregulated, practices will be adopted. For example, regulating telephone tapping but not the bugging of premises may be expected to increase the incidence of the latter, more intrusive, activity:

> "*Once one form is subject to legal regulation, failure to control other forms not only becomes morally indefensible, but also in practice undermines the protection granted. This arises from the simple behavioural prediction that, assuming equal effectiveness, measures that can be undertaken free of oversight will be much more attractive to people doing the work than those which are subject to review.*"[25]

42. Cost is also a factor governing the relative incidence of different categories of surveillance techniques. Telecommunications interception is a favoured method of surveillance because it is comparatively cheap.[26] All surveillance techniques have as their object the obtaining of information that is not forthcoming through overt methods. The method chosen will depend on legal, logistical and financial considerations.

An integrated approach to regulating intrusion

43. These factors indicate that an integrated approach should be adopted to the regulation of intrusions upon privacy. Protection against undue interference with privacy is effective only if interception of communications as well as some other forms of surveillance are regulated. We consider that the United Kingdom approach, which regulates only interception of telecommunications and mail, is therefore unsatisfactory.

44. As covert methods vary in their degree of intrusiveness, an integrated approach could stipulate that a more intrusive method be resorted to only when a less intrusive one is not practicable. For example, techniques which involve physical intrusion into premises (such as planting a recording device) may be more intrusive than electronic surveillance conducted by remote means. This approach would have the added advantage of avoiding problems of definition which arise if an attempt is made to regulate only some surveillance activities.

---

25 Lustgarten and Leigh, *op cit,* at 44.

26 This was confirmed by the Australian Barrett Review in 1994, which estimated that such interception costs AUS$570 a day, compared with AUS$1,376 for optical surveillance, $1,630 for listening devices, AUS$1,895 for physical surveillance, or AUS$2,772 for vehicle tracking. See P J Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception*, (Department of Finance, March 1994), chapter 6.

The privacy debate in Hong Kong

45. A number of reports have been released in the last five years focusing on telephone interceptions in Hong Kong. In 1991, Justice released a report seeking the introduction of legislation requiring telephone interceptions to be justified to an independent body. In March 1991, the Bar Association prepared a submission to the United Nations Human Rights Committee on the Third Periodic Report on Hong Kong. The submission addressed the issue of telephone tapping and argued that there is "no clear legal authority for this practice". They added that there was a:

> *"complete lack of information on who could authorize telephone tapping, under what circumstances it could be authorized, and what safeguards are there to prevent abuse or unjustifiable invasions of privacy."*[27]

46. On 5 April 1991, the *South China Morning Post* reported that the Human Rights Committee had questioned government representatives on the issue and called for additional legal protections.

47. On 26 May 1992, the same paper reported that the Convenor of the Omelco Constitutional Development Panel, the Hon Andrew Wong, had said that the reference in section 33 of the Telecommunication Ordinance (Cap. 106) to tapping in the "public interest" required to be more clearly defined. More recently, the Review Committee of the Independent Commission Against Corruption recommended a review of existing powers to intercept communications.

48. A further recent development was a proposal to introduce a private member's bill to impose a court warrant system to regulate the interception of telecommunications and mail.[28]

Local attitudes

49. The differences in attitude to privacy between countries, and even between different sections of the same community, is acknowledged by commentators. A survey conducted by Drs John Bacon-Shone and Harold Traver in Hong Kong in 1993 included a number of questions addressing surveillance.[29] The questions and responses are set out below:

---

27 Para. 7.4.21.

28 *South China Morning Post,* 6 August 1995; *Hong Kong Standard,* 17 April 1996.

29 A summary of the results of the survey can be found in: Law Reform Commission of Hong Kong, *Report of the Law Relating to the Protection of Personal Data* (1994), Appendix 2.

1.	*Q.*	*Recently a building has been built so close to yours, that people in it can easily see what you are doing in your living room. Do you take this as a serious matter?*
	A.	No concern at all ("NCAA"): 12.5%; Little concern ("LC"): 22.5%; Very concerned ("VC"): 56.4%; Extremely worried ("EW"): 8.5%. **[VC/EW: 64.9%]**
	Q.	*Do you think that it is necessary that this should be controlled or limited by law?*
	A.	**Yes: 64.8%;** No: 29.4%; Don't know: 5.8%.
2.	*Q.*	*Someone uses a camera with telephoto lens to take a picture of you in your house without your knowledge or consent. Do you take this as a serious matter?*
	A.	NCAA: 5.4%; LC: 7.1%; VC: 68.2%; EW: 19.3%. **[VC/EW: 87.5%]**
	Q.	*Do you think that this should be controlled or limited by law?*
	A.	**Yes: 85.8%;** No: 12.1%; Don't know: 2.1%.
3.	*Q.*	*You discover that your employer has been opening mail sent to you marked "personal". Do you take this as a serious matter?*
	A.	NCAA: 3.7%; LC: 9.7%; VC: 73.7 %; EW: 12.9%. **[VC/EW: 86.6%]**
	Q.	*Do you think it is necessary that this should be controlled by law?*
	A.	**Yes: 76.5%;** No: 20.0%; Don't know 3.5%.

4.	*Q.*	*You read in the newspaper that in order to combat crime the police are seeking the power to tap the phones of anyone they suspect of committing a crime. Do you take this as a serious matter?*
	A.	NCAA: 26.5%; LC: 30.8%; VC: 39.1%; EW: 3.6%. **[VC/EW: 42.7%]**
	Q.	*Do you think it is necessary this should be controlled by law?*
	A.	**Yes: 53.5%;** No: 37.1%; Don't know: 9.4%.
5.	*Q.*	*Recently, private telephone conversations are being reported publicly in the newspaper to attract readers. Do you take this as a serious matter?*
	A.	NCAA: 26.0%, LC: 31.2%; VC: 39.3%; EW: 3.6%. **[VC/EW: 42.9%]**
	Q.	*Is it necessary this should be controlled by law?*
	A.	**Yes: 67.9%;** No: 26.2%; Don't know: 6.0%.

In response to each question, over 50% thought that legal regulation was called for. A similar survey carried out in 1996 did not show any material change to the results.

A broad approach to protection from intrusion

50. We have concluded that our initial task should be to define clearly the scope of the individual's right of protection against intrusion. Only once that is done can the scope of legal controls be examined. The purpose of surveillance is the capture of information relating to the individual, but the intrusive nature of the process means that surveillance is objectionable whether or not any information is obtained as a result.

51. The individual's reasonable expectation of protection from intrusion should not be adversely affected by "bad" practices in society. Intrusions may be commonplace in Hong Kong but this should not preclude an individual from expecting minimum standards set out in the International Covenant buttressed by the provisions of the Basic Law. The decisions of the

European Court of Human Rights in *Klass*[30] and *Malone*[31] indicate that the relevant standard is what an individual should be entitled to expect in a society governed by the rule of law. This reasonable expectation should be judged objectively according to the standards of a society subject to the rule of law. In the Hong Kong context, this means that the individual should have a right to expect that the protection afforded to his privacy be measured up to the minimum standards enshrined in the ICCPR and the Basic Law. To proceed in any other way would mean that the rights of the individual under the ICCPR could be ignored or diminished by their negation in practice. This would be incompatible with the notion of the rule of law.

52. Distinctions are often drawn between aural and visual surveillance. In principle, we consider such distinctions to be irrelevant. It should not matter what perceptual sense is employed by the intruder. Whilst telephone calls may be overheard, letters may be read and significantly communicative non-verbal behaviour monitored. Similarly irrelevant, in our opinion, is whether the data collected is immediately meaningful to the recipient; infrared signals signify the presence of a human being as much as photographic images.

53. A person's reasonable expectation of privacy can be broadly categorised as follows:

a) that he will not be deliberately observed or overheard; or

b) that he will not have his communications deliberately intercepted, read, or recorded; or

c) that he will not have his personal, professional or business articles, data and papers deliberately examined, copied or recorded,

when in all the circumstances he has a reasonable expectation that the intrusion in question will not occur.

54. This classification distinguishes between the capture of data that directly emanates from the individual (such as appearance, sound, temperature and odour), which is addressed by (a), and data that is instead consciously generated by the individual (such as on his word processor), which is addressed by (c). While the latter category of data is already partly addressed by the Personal Data (Privacy) Ordinance and the anti-hacking provisions of the Telecommunication Ordinance, the former is at present totally unregulated.

55. Insofar as the individual has a reasonable expectation of privacy in the use of certain communications, he is entitled to have, in accordance with the ICCPR, an expectation that the privacy of such communications will

---

30 (1974) 2 EHRR 214.
31 (1984) 7 EHRR 14.

be governed by the rule of law and that the law will protect such communications from any arbitrary or unlawful interference.

General approach to criminal sanctions

56. Having briefly considered the individual's right to, and expectation of, privacy, we now address the difficult issue of what conduct which infringes this expectation should be subject to criminal sanctions. This is distinct from the issue of whether a civil remedy should be available.

57. In framing recommendations on criminal sanctions we have been guided by the following principles:

a) *Social need*: In determining the scope of criminal sanctions, we should not criminalise conduct unless it is essential to do so. Social need is a crucial consideration and a law that does not reflect society's views will be ignored. The adequacy or otherwise of the present law is relevant to whether criminal sanctions are required. A danger of broadly drawn criminal offences is that they could lead to abuse.

b) *Establishing norms*: The imposition of criminal sanctions usefully establishes social norms to proscribe clearly unacceptable conduct.

c) *Deterrence and retribution*: Establishing a criminal offence also acts as a deterrent. This would be so even if no prosecution were ever brought.

d) *Systematic investigations*: Attaching criminal sanctions to unacceptable conduct provides the individual with police assistance in investigating and remedying wrongdoing.

58. Having carefully considered the issues, we agree that criminal sanctions are necessary to regulate intrusion upon privacy. As far as the interception of communications is concerned, the detailed arguments supporting this conclusion are provided in chapter 4 below.

Consultation paper

59. On 16 April 1996, the Privacy sub-committee issued a consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*. The consultation period lasted for two months and ended on 15 June 1996. The sub-committee received over 30 submissions. We are grateful to all those who commented on the consultation paper. A list of those who responded is at the Annexure.

60. After briefly considering all the submissions from the respondents, the sub-committee decided that priority should be given to finalising the recommendations on the interception of communications and that their report to the Commission should be split into two parts, the first dealing with interception of communications and the second with surveillance involving intrusion into private premises.

61. It is clear from the submissions that it is the procedure under section 33 of the Telecommunication Ordinance (Cap. 106) that has aroused most public concern and pressure for change. In fact, it is fair to say that most, if not all, respondents agree that there should be provisions regulating the interception of communications. There is little controversy over the proposal that the existing procedure should be replaced by a warrant system under the scrutiny of a judge. In order to enable the Administration to respond swiftly to such demands, we agreed to defer our deliberations on the regulation of surveillance and to focus first on issues concerning interception of communications. This report therefore deals mainly with interception of communications.[32] The sub-committee will resume the discussion relating to intrusion into private premises shortly after we have finished our deliberations on this report.

Sub-committee meetings

62. The Privacy sub-committee started discussing the second part of the privacy reference on 11 February 1995. A total of 26 meetings were held to arrive at the conclusions and recommendations in the consultation paper. Another 21 meetings were held to discuss the comments received from those responding to the consultation paper.

Responses to the consultation paper

63. The overwhelming majority of those who responded to the consultation paper, including the law enforcement agencies, supported the proposal that interception of communications should be regulated by law. A few expressed the concern that our recommendations would affect the private sector as well as the public authorities. There were also suggestions that the media should be exempted from regulation and that a public interest defence should be available to the person charged with the proposed interception offence. All these concerns are addressed in this report.

64. We have taken into consideration all the comments received by the sub-committee. Our approach is to concentrate on the basic principles which would help shape a regulatory framework which is both feasible and

[32] To be more precise, this report deals mainly with the interception of telecommunications and mail. The regulation of the interception of communications by means of a technical device will be covered by the report on surveillance. See chapter 4 below.

broadly acceptable to the public. The technical details of the proposals would be a matter for the Administration and the law draftsman at a later stage.

Chapter 1

Interception of communications: technical aspects

Summary

1.1 The privacy of communications is already subject to legal controls, not all of which are consistent. These are examined in the following two chapters. Before examining these controls, the ways in which interceptions are effected in modern telecommunications systems is summarised. These are as varied as the telecommunications systems now employed. Since 1993, Hong Kong has had a fully computerised digital communications infrastructure. This replaced an analogue system which was susceptible to wiretaps. However, in a digital system interceptions can be effected remotely by manipulation of the computer switching software. Hacking into this software via on-line PC's has been reported in other jurisdictions. Mobile communication systems, which are based on radio signal transmissions, are vulnerable to interception via computer based scanners.

1.2 Modern computer techniques facilitate the interception of only those communications of particular interest. Programs to assist the interceptor in targeting intercepts include those that recognise particular voices, key words or phrases, or specific telephone numbers.

Introduction

1.3 Modern telecommunications systems are either analogue or, more recently, digital. The technical position is summarised by Fitzgerald and Leopold as follows:

> "*In a conventional telephone network, the sound of the human voice is converted into an electrical current, which takes a form analogous to* the *speech pattern; as the sound of the voice on the telephone changes, so does the shape of the electrical signal on the line. ... In a digital transmission system, on the other hand, sound is converted into a series of bits [binary digits] ... . In a digital system, data is encoded as strings of '0's and '1's, which, in a computer, are represented by the presence*

or absence of electrical pulses ... each string of digits corresponding to a particular voice sound level."[1]

1.4 It is not only the human voice which can be encoded into bits and transmitted in digital form; so too can computer data:

"Computer data may be transmitted, just like telephone signals, down cables or over high frequency microwave radio systems. Over long distances, it is usually sent along normal telephone lines, after being changed, by a device known as a 'Modem' (MOdulator/DEModulator), out of its digital, on-off, form into a wave-like signal which can be carried by the analogue telephone network we currently enjoy [i.e. in the UK in the late 1980s - all of the Hong Kong system is digitalised]."[2]

1.5 Just as computers have become increasingly efficient, so have modems, with affordable models small enough to carry with a notebook, and capable of being run off a battery pack. Computer data already comprise half the traffic on a telephone network and the proportion is increasing: data income is growing six times as fast as voice income.[3] Fitzgerald and Leopold continue:

"Intercepting computer data can be done in one of two ways. If it passes through the phone system, or even a direct wire, it can be picked up by any of the normal amateur phone tapping methods, although naturally the snooper needs a suitable terminal, rather than a telephone handset, to make the signal intelligible. ...

More common than computer tapping is hacking. A computer which can be dialled up on the telephone to allow its legitimate users to communicate with it from a distance may also be accessed by anyone with a computer and modem who wants to find out what is in the memory. The hacker needs to understand how to control the computer they have accessed, and most large organisations try to keep their data secret by restricting access to those who have an authorised user identity code and one or more passwords. Only when these are fed into the central processing unit (CPU) will the computer allow access to its memory."[4]

1.6 As explained above, "hacking" is a pejorative term used to denote *unauthorised* access to a computer. For the purposes of the present discussion, lack of authority is not the point. What *is* fundamental is that the distinction between computers and telephones has become blurred. The

---

1 P Fitzgerald and M Leopold, *Stranger on the Line: The Secret History of Phone Tapping* (London: The Bodley Head Ltd, 1987), at 222 and 226.

2 *Ibid,* at 223.

3 *The Economist,* 16 October 1993.

4 Fitzgerald and Leopold, *op cit,* at 223-224.

switching systems of modern digitalised telephone systems are controlled by computers and interception is effected by manipulation of the software on which those computers completely depend. Each telephone number is represented by a long code, the LEN (Line Equipment Number), which assigns functions and services such as "call forwarding" to the phone. Switching manipulation of the codes may re-route calls, re-assign numbers or effect other alterations. It would allow the eavesdropper to listen in on the switch routed call. Because computers can talk to each other through the use of modems, manipulation of switching software may be effected on the computer in question or through another computer anywhere in the world. It might be for law enforcement purposes, or it might be hacking for fun. Again, it may be for profit. For example, a credit card thief may re-route verification calls from the credit card company to a number to which the thief has access. As Clough and Mungo put it, a telephone network is "really just a giant computer linking terminals - or telephones - with switches and wires and loops all across the country".[5] We could add that he could now have said "across the world".

1.7 Furthermore, as Fitzgerald and Leopold point out, digitalisation makes telephone tapping less detectable:

> *"In its essence, all conventional tapping consists simply of attaching an extension telephone to the target's line. Whether this is done at the exchange by professionals or by the methods described in Chapter 8, there is always a physical tap somewhere on the target's line which can be seen, if not by the tapped person then by [British Telecom] engineers. ... Digital tapping is different. The tap leaves no physical presence anywhere; it is literally invisible, and makes no discernable changes to the telephone circuit being tapped."*[6]

1.8 In the days of analogue telecommunications, non-intrusive monitoring at the subscriber's copper loop was easy; a simple device could intercept all required information. In contrast, retrieving the bit stream from the same pair of copper wires carrying digital information requires high technology equipment that can handle the many different local switching systems now in use. A similar increase in complexity applies to the wireless environment. Increased use of air waves and new transmission and coding schemes all demand high technology solutions.

Mobile phones: interception of radio signals

1.9 Tapping and manipulation of computer software are two of the main methods of effecting the interception of telecommunications. A third method is by means of the interception of radio channels. These may be terrestrial or, for international communications, by means of satellite. Those

---

5 B Clough and P Mungo, *Approaching Zero: Data Crime and the Computer Underworld*, (London: Faber & Faber, 1992), p.12.

6 *Ibid,* at 227 - 228.

who still use analogue portable phones are particularly vulnerable. As an article in the International Herald Tribune put it, calls can be intercepted by anybody with a radio frequency scanning device "as easily as a motorist tunes into a station on a car radio". This is particularly so if the call is made on the street:

> *"Cellular telephones are radio transmitters that broadcast to and receive signals from a network of 'cells' or transmission towers. When a cellular user drives or walks, different cell sites capture and strengthen the cellular telephone's radio signal and then connect the phone to the regular telephone network."*[7]

1.10 The article goes on to point out such radio frequencies have difficulty penetrating thick walled buildings. But interceptions may still be effected by devices registering the vibrations off windows.

1.11 Cellular phones using analogue signals are easy to listen to because they broadcast the sound of the human voice. Conversations on such phones can be encrypted, but only with an elaborate and expensive model of phone. Digital models, on the other hand, code the voice in numbers, making them readily encrypted and, until recently, less susceptible to eavesdropping. Analogue systems have been scanned via computer based radio scanners locked onto a particular cell site (a micro broadcasting/receiving radio station atop a building, etc). The hacker scans the analogue transmission from cell site to cell site. With digital (e.g. GSM) systems scanning is inherently more difficult. The digital signal encryption is based on an algorithm and a high speed array processor computer is required to crack the code. However, it is not clear whether personal communications service will be encrypted.

1.12 There is a recognition that the Telecommunication Ordinance (Cap. 106) does not adequately address the interception of mobile phone calls. As one official explained:

> *"When we drafted that ordinance in 1963 we were looking at a telecommunications industry that was basically restricted to a wire telecommunications network".*[8]

International interceptions

1.13 International telecommunications transmissions are made by means of satellite or cable. Fitzgerald and Leopold explain the technical aspects:

> *"The telecommunications satellite acts as a relay station, amplifying and retransmitting the signals which it receives, so*

---

7 *International Herald Tribune,* 23 June 1992.

8 *South China Morning Post,* 12 May 1994.

that all earth stations within sight of it can exchange transmissions with each other. ... Shadow earth stations are adequate for intercepting one-way telex or data transmissions, through which much international trade is conducted, but there comes a problem in dealing with telephone or duplex (simultaneous, both-way) data traffic. The two parts of the conversation must be intercepted on different channels or, in some cases, even at different monitoring stations. Moreover, a large proportion of international communications travels via cable ... . Cables are inherently more resistant to tapping than radio links ... . Despite the difficulties, it is possible to tap underground and submarine cables [by means of devices that] detect the magnetic field around the target line, caused by the current flowing through it, which can be analysed to reveal the traffic on that line."[9]

Analysis of transmissions

1.14 Fitzgerald and Leopold point out that:

"The values of tapping has always been depressed by the need to sort through the intercepts to distill useful intelligence from a mass of trivia. This is a tedious, painstaking process better suited to computers than to human analysts. "[10]

1.15 They describe the following computer strategies aimed at sifting out material of possible interest:

- Filtering out spurious traffic on the basis of call destinations.
- Keyword recognition: programs register the occurrence of a particular word in a conversation, regardless of who says it.
- Voice recognition:

  "This is likely to be more productive than key word recognition: targets of tapping are frequently circumspect in what they say on the phone, but the presence of a particular speaker cannot be disguised - false accents will not fool the system."[11]

  "Such a system could, for example, be used to trawl out all international calls made from any telephone by a particular political activist."[12]

---

9 Fitzgerald and Leopold, *op cit,* at 95 - 96.
10 *Ibid,* at 73.
11 *Ibid,* at 111.
12 *Ibid,* at 107.

1.16 Fitzgerald and Leopold caution, however, against the assumption that it is only mavericks who may be tapped:

> *"Even people who may themselves be above suspicion of being subversive or engaged in serious crime may be tapped, because of what they know, or because of what they may have been told. The fact that the Left are the most vocal on the subject of tapping should not convince others that they themselves are not tapped. In many ways, the VIP denizens of Westminster and the City of London are far more likely to be of interest to the intelligence world than is the average would-be agitator."*[13]

Message systems of telecommunications systems

1.17 A comprehensive account of interception of telecommunications requires mention of the interceptability of modern message systems.

Facsimile

1.18 Faxes are vulnerable to interceptions, particularly the telephone lines that service machines: "The wires going into faxes are exposed at least once or twice on each floor of a building, it's terribly easy to wiretap" according to former IBM computer security chief Mr Robert Courtney.[14] Alternatively, a fax message may be intercepted during transmission by telephone lines, unless adequately encrypted. At the destination, the hard copy is like an open envelope and is vulnerable, particularly if messages are concentrated through shared machines.

Electronic mail

1.19 Computerised messaging networks enable desktop computers to talk to one another. The sender types a note on his computer screen and by pushing the "send" button transmits it to another person's computer screen. Electronic mail has been described as the modern equivalent to sending a letter through the mail without an envelope:

> *"Picking off E-mail could be just as simple as re-programming the circuit board that connects the machine to the company network, said Stanford University Professor Martin E. Hellman, an electronic message security expert. Tell it to ignore the address that was at the front of each message, he said. With sorting by address turned off, every piece of mail that went*

---

13 *Ibid,* at 31.

14 Quoted in *South China Morning Post* 20 February 1990.

through the network could be dumped into that machine's memory. Then, the internal spy could narrow down his search fairly easily, he said. The mail can be sorted by key words, to pull up items of interest. Addresses of particular recipients can be extracted and then used. So, if a worker really wants to see what the boss thinks, it was a matter of pulling out all the boss' mail and searching for one's own name."[15]

1.20 In 1986 the United States Congress enacted the Electronic Communications Privacy Act to provide electronic messages on telecommunications systems the same protection from disclosure as telephone voice messages.[16] However, this is an area where social and legal norms have not kept up with new technologies. Anne Wells Branscomb comments:

"However, this law would not be applicable to corporate messaging systems where authorized managers enter what may be perceived as personal electronic files. And here is where the law and the expectations of employees became muddled."[17]

1.21 She cites a recent *Macworld* survey of "electronic eavesdropping" reporting that 41.5% of the 301 participating companies admitted searching the electronic mail of employees. Only 30.8% of the companies gave advance warning to employees.

1.22 A technical aspect of electronic mail which may require legal recognition is that its intended "deletion" may be ineffective. In a review of how e-mail is being increasingly utilised in litigation as evidence, the Asian Wall Street Journal reports that while most systems only keep such messages readily retrievable for, say, five days:

"To the surprise of many defendants, even deleted information can be resurrected. Telling a computer to delete something is the same as saying to it, 'it's OK to write over this.' But the computer might not do so for years, and then might overwrite only parts of the information. Until it is overwritten, the deleted information actually remains in the computer and can be retrieved by programmers."[18]

1.23 In the United States a major court decision recognised how much business is now conducted on the computer. In August 1993, the United States Court of Appeals for the District of Columbia held that the United States government must preserve e-mail under the same standards as applied to paper communications. The Clinton administration had argued that

---

15 *South China Morning Post,* 3 May 1994.

16 The 1986 Act amends the Omnibus Crime Control and Safe Streets Act of 1968.

17 *Who Owns Information?* (Basic Books, 1994), p. 94.

18 *Asian Wall Street Journal,* 6 January 1993.

it was sufficient if officials were encouraged to make print-outs of what was on their computer screens, but the Court rejected this argument:

> *"The Government's position is basically flawed because the hard-copy printouts that the agencies preserve may omit fundamental pieces of information which are an integral part of the electronic records, such as the identity of the sender and/or recipient and the time of receipt."*

Hong Kong's telecommunications industry

1.24 The regulation of the telecommunications industry in Hong Kong falls under the responsibility of the Telecommunications Authority appointed under the Telecommunication Ordinance (Cap. 106).[19]

1.25 Before July 1995, local public wire-line voice telephone services were provided by the Hong Kong Telephone Company Limited under an exclusive concession granted under the Telephone Ordinance (Cap. 269). Following a review of telecommunications policy in 1992, the Government decided to introduce competition to the fixed network market. On 1 July 1995, four new Fixed Telecommunication Network Services licences were issued for providing local telephone service on a competitive basis.[20] Each of the four licences lasts for 15 years and is renewable for another 15 years. The operators can also offer public switched facsimile and data services on a competitive basis.

1.26 The Office of the Telecommunications Authority Trading Fund Report 1996[21] provides the following information and statistics on the telecommunications industry as at 31 March 1996:

(a) Hong Kong's telecommunications industry had a turnover of HK$39 billion in 1995-96.

(b) Hong Kong had the highest per capita density of telephones in Asia outside Japan with a penetration rate of 68 telephones and 52 exchange lines per 100 persons.

(c) The levels of penetration in the various mobile communications in Hong Kong match, and in many cases exceed, those achieved elsewhere around the world.

(d) There were four licensed cellular phone operators in Hong Kong. They operated five digital and three analogue systems serving a total of

---

19 The Office of the Telecommunications Authority ("OFTA") hived off from the Telecommunications Branch of the Post Office on 1 July 1993. It then established itself as an independent government department.

20 The 4 licences were issued to the Hong Kong Telephone Company Ltd, Hutchison Communications Ltd, New T & T Hong Kong Ltd and New World Telephone Ltd.

21 OFTA, *Office of the Telecommunications Authority Trading Fund Report for the period 1 June 1995 to 31 March 1996*.

about 800,000 customers. The number of CT-2 customers declined rapidly as cellular phone services became more popular.

(e) The Government decided in 1994 that up to six Personal Communications Service licences and up to four Cordless Access Service licences in the 1.7 - 2.0 GHz band would be issued.[22]

(f) There were 31 operators licensed to provide public radio paging services. The per capita subscription rate was one pager for every six people in the population.

Eavesdropping in Hong Kong

1.27 As mentioned above, the government does not presently provide figures on the number of telephone interceptions carried out, nor, of course, does the private sector. However, the *Sunday Morning Post* reports that private investigation companies are busy unearthing secret listening devices. The most frequently found culprits are hard wire taps, where a short wire is attached to the target's telephone line anywhere in the building.

[22] The Telecommunications Authority expects to issue 6 Personal Communications Service licences in 1996-97.

Chapter 2

Statutory regulation of communications

Summary

2.1 This chapter examines the existing statutory controls on the interception of communications. These are contained in the Telecommunication Ordinance (Cap. 106) and the Post Office Ordinance (Cap. 98). We first examine the relevant provisions of the Telecommunication Ordinance. There are several offences prescribed:

- *Section 27 prohibits interference with a "telecommunication installation" with intent to intercept or discover the contents of a message.*
- *Section 8 prohibits the possession or use of scanners and receivers without a licence.*
- *Section 27A prohibits unauthorized access to any program or data held in a computer.*

2.2 Under section 33, the Governor may, if he considers that the public interest so requires, order that:

- *any message brought for transmission shall not be transmitted; or*
- *any message brought for transmission, or transmitted or being transmitted, shall be intercepted or disclosed to the Government.*

The question of the compatibility of section 33 with the International Covenant on Civil and Political Rights will be discussed in the next chapter.

2.3 Turning to the interception of mail, we briefly examine the provisions of the Post Office Ordinance addressing this, including section 13 which empowers the Chief Secretary to grant a warrant authorising the Postmaster General to open and delay any postal packet. The powers in section 13 are broader than those of its counterpart in the Telecommunication Ordinance.

Regulation of telecommunications[1]

Interference with telecommunication equipment

2.4 The Telecommunication Ordinance (Cap. 106) provides for the authorisation of interceptions, but its only general prohibition of interceptions *without* authority is section 27. This provides:

> *"Any person who damages, removes or interferes in any way whatsoever with a telecommunication installation with intent to -*
>
> *(a) prevent or obstruct the transmission or delivery of a message; or*
>
> *(b) intercept or discover the contents of a message,*
>
> *shall be guilty of an offence and shall be liable on summary conviction to a fine of $20,000 and to imprisonment for 2 years."*

"Telecommunication installation" is defined as meaning "any apparatus or equipment maintained for or in connection with a telecommunication service".

2.5 This provision does not appear to have been the subject of authoritative judicial consideration. It has seldom been the subject of a prosecution, although a magistrate recently held that this provision applied to a defendant who effectively disabled a fax machine by sending over 80 pages a day of unwanted faxes. The statutory language is not particularly effective to cover the interception of *telecommunications*, as opposed to interference with telecommunication equipment. This is also the case with regulation 9(1) of the Telecommunication (Control of Interference) Regulations (Cap. 106, sub. leg. A) by which a person commits an offence if he "uses any apparatus for the purpose of interfering with the working of any apparatus for telecommunication". However, the interception of telecommunications is designed *not* to interfere with the working of the apparatus, so as to avoid detection.

Licensing of scanners and receivers

2.6 Section 8 of the Telecommunication Ordinance makes it an offence, without a licence, to:

---

[1] Subsequent to a review of the Telecommunication Ordinance, the Office of the Telecommunications Authority issued a consultation paper in August 1996 proposing amendments to the Ordinance. The purpose of the amendments is three-fold: (a) to regulate operators of Public Telecommunication Services, in particular to incorporate provisions in the Fixed Telecommunication Network Service licence into the Ordinance; (b) to provide the Authority with statutory powers to manage the radio spectrum and to prevent interference with telecommunication service; and (c) to update and consolidate the existing provisions in the Ordinance. These proposed amendments have no direct implications on our recommendations.

"(a) establish or maintain any means of telecommunication; or

(b) possess or use any apparatus for radiocommunication or any apparatus of any kind that generates and emits radio waves notwithstanding that the apparatus is not intended for radiocommunication; or [to deal in the course of trade or business in such apparatus]."

2.7 The *South China Morning Post* reported on 30 August 1992 that "a wide variety of scanners and receivers are available in Hong Kong, some for as little as $650, most being sold on the understanding the buyers are tourists and the equipment will be exported."[2] Portable handheld radio scanners can be easily concealed in a coat pocket. Police have reportedly discovered transceivers tuned to police radio bands in the course of raids.[3] The concern that criminals were able to monitor police movements prompted the Telecommunications Authority in 1994 to increase financial penalties ten fold (to $100,000) under the Telecommunication Ordinance. A prison term of up to five years remains prescribed.[4] In 1993, the police reported that they had been "unable to find a technical solution to the problem" and accordingly sought a tightening of the licensing of telecommunication equipment.[5]

2.8 The interception of communications may also be effected by equipment which does not have eavesdropping as its primary function. For example, a radio is able to pick up police conversations.

Hacking

2.9 "Hacking" is the unauthorised access to data or programs held in a computer. The telephone system allows computers to "talk" to each other. The hacker issues commands on his own computer identifying the database number of the other computer (which may be unlisted) and these are transmitted through the phone network. This transmission is effected by converting the computer commands by means of a modem to signals that can be transmitted by the phone network. The receiving computer's modem converts the signals back into computer commands. Hacking has clear privacy implications:

> "*One of the favourite targets for hackers in the US is the TRW system, the nation-wide credit agency that holds financial information on some 80 million Americans, and in the mid-1980s hacking TRW was reputed to be so simple it was almost routine. A hacker named 'Michael Synergy' once broke into the agency to have a look at then-president Ronald Reagan's files. He*

---

2 Possession of radiocommunication apparatus purchased by visitors in Hong Kong is exempted from the requirement to hold a licence under section 8 of the Telecommunication Ordinance: Telecommunication (Possession and Export of Radiocommunication Apparatus by Visitors) (Exemption) Order (Cap 106, sub leg O).

3 *Hong Kong Standard,* 8 October 1993.

4 Cap 106, section 20.

5 *South China Morning Post,* 11 October 1993.

located the files easily, and discovered sixty three other requests for the president's credit records, all logged that day and all from unlikely sources."[6]

2.10 A commonly employed technique for effecting the interception of communications is hacking. Accessing a computer's programs requires the user to key in the appropriate account number, ID (or "log-in"), and password, but there are various methods of obtaining these. One is guesswork: people pick simple combinations for the obvious reason that they need to remember them. Another arises from the fact that:

"*When computers are manufactured a number of default log-ins and passwords are programmed into the machines. A common one is 'sysmaint', for systems maintenance, used as both the log-in and the password. Accessing a machine with this default would require no more than typing 'sysmaint' at the log-in prompt and then at the password prompt. Computer operators are supposed to remove the default access codes when they take delivery of the computer, but many forget or don't bother."*[7]

2.11 The FBI estimates that computer-related crime costs the United States between US$500 million and US$5 billion per year. Price Waterhouse now provides "hired hackers" for testing the security of company information systems.

2.12 In Hong Kong, no research has been done on quantifying the likely extent of hacking in the territory. It is reported that this will be one of the first tasks of the Police's Crime Prevention Bureau Special Projects Unit, recently established to complement the enforcement role of the Commercial Crime Bureau.[8]

2.13 Hacking is now (partly, see below) addressed by section 27A of the Telecommunication Ordinance. This provides:

"(1) Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $20,000."

2.14 Section 2 defines "telecommunication" as:

"any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by visual means or by wire or radio waves or any other electromagnetic system."

---

6 *Approaching Zero, op cit,* at 59.

7 *Ibid,* at 64.

8 *South China Morning Post,* 30 October 1995.

2.15 Two people have been successfully prosecuted under this section to date. In 1994, a travel agency employee was fined $15,000 for hacking into a competitor's database and, in a high profile prosecution in April 1995, a computer enthusiast was convicted of hacking into the databases of two Hong Kong educational institutions.

2.16 In *R v McLaughlin,*[9] the Canadian Supreme Court held that a similar provision would not catch unauthorised access to a computer which was not effected by *another* computer. The court commented:

> *"The term 'telecommunication' as defined in the Criminal Code connotes a sender and a receiver. The computer, being a computing device, contemplates the participation of one entity only, namely the operator. In a sense, he communicates with himself, but it could hardly be said that the operator by operating the terminal or console of the computer is thereby communicating information in the sense of transmitting information and hence it stretches the language beyond reality to conclude that a person using a computer is thereby using a telecommunication facility in the sense of the Criminal Code."*[10]

2.17 Press reports indicate that a similarly restricted application of the Hong Kong Ordinance was intended. For example, the *South China Morning Post* quotes a government spokesman as saying that the aim of the legislation is to prevent illegally accessing a computer system from a remote location by means of a modem and a telephone.[11]

2.18 This deficiency in section 27A of the Telecommunication Ordinance is, to some extent, remedied by section 161(1) of the Crimes Ordinance (Cap. 200) which provides that:

> *"Any person who obtains access to a computer -*
>
> *(a) with intent to commit an offence;*
> *(b) with a dishonest intent to deceive;*
> *(c) with a view to dishonest gain for himself or another; or*
> *(d) with a dishonest intent to cause loss to another,*
>
> *whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years."*

2.19 It appears that there have been only two convictions under section 161(1) since its enactment in 1993.

---

9 (1980) 53 CCC (2D) 417.

10 *Ibid, at 425.*

11 *South China Morning Post,* 27 March 1992. The United Kingdom position is different. Section 1 of the Computer Misuse Act 1990 provides that a person commits an offence if without authority "he causes a computer to perform any function with intent to secure access to any program or data held in any computer". See *Attorney-General's Reference (No. 1 of 1991)* [1992] 3 All ER 897.

Authorising interception of telecommunications

2.20 Section 33 of the Telecommunication Ordinance provides for an authorisation process in the following terms:

> *"Whenever he considers that the public interest so requires, the Governor, or any public officer authorized in that behalf by the Governor either generally or for any particular occasion, may order that any message or any class of messages brought for transmission by telecommunication shall not be transmitted or that any message or any class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication, shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order."*

2.21 We examine in the next chapter the human rights jurisprudence on interception of communications. Suffice to say at this stage that section 33 may not reflect the provisions of the ICCPR and the Basic Law.

2.22 The operation of section 33 was the subject of a Legislative Council question on 11 November 1992. The Hon Gilbert Leung asked:

> *"Will the Government inform this Council of the total number of orders made under the Telecommunication Ordinance for tapping private telephone conversations in the past three years; and whether the Administration has conducted any review, since the Hong Kong Bill of Rights Ordinance came into effect last year, of such tapping activities undertaken by the departments concerned to ensure that the provision on the protection of privacy as stipulated in article 14 of the above Ordinance could be complied with?"*

2.23 The Secretary for Security replied:

> *"Orders under s. 33 of the Telecommunication Ordinance to intercept telephone transmissions are made only when the public interest so requires and only in cases involving the prevention or detection of serious crime, including corruption, or in the interests of the security of Hong Kong. Such orders are authorised by the Governor, who has to be satisfied personally that these criteria are met. It would not be appropriate on law and order and security grounds to disclose details of orders made, including numbers. However, members can be assured that all applications submitted and decisions made are considered carefully on their merits.*
>
> *I can confirm that we are looking at our legislation to see if it is in need of modernisation in the light of the introduction of the Bill*

of Rights, and a review is now underway. In this review we will carefully take into account the recommendations of the Law Reform Commission, which is presently examining existing Hong Kong Laws affecting privacy, including the interception of communications."

2.24 Whilst the Secretary for Security declined to give figures, a recent indication that tapping is increasing is provided by press reports that the Independent Commission Against Corruption has installed extra equipment and hired ten additional staff to enable it to increase its tapping capability from 50 to 80 lines.[12]

Regulation of mail

2.25 In addition to telecommunications, controls on postal communications are directly relevant to our reference. The regulation of postal services provided by the Post Office is addressed by the Post Office Ordinance (Cap. 98). That Ordinance contains considerably more elaborate provisions for the interception of "postal packets" than the comparable provisions of the Telecommunication Ordinance. "Postal packet" is defined in section 2 as "a postal article, or a collection of postal articles, which is in the course of transmission by post as one postal unit." "Postal article" is defined in the same section as "includ[ing] everything which is transmissible by post." The Ordinance defines a number of offences safeguarding mail delivery.

Offences under the Post Office Ordinance

2.26 The Ordinance prohibits the following:

(a) wilfully opening any postal packet addressed to some other person or doing anything whereby the due delivery of any postal packet addressed to some other person is prevented or delayed, either with intent to injure such other person or with intent to obtain some benefit for himself;[13]

(b) fraudulently retaining, or wilfully secreting or keeping or detaining any postal packet;[14]

(c) without lawful authority or excuse,
- opening or delaying any postal packet;
- taking any of the contents out of any postal packet; or
- having in his possession any postal packet or any contents thereof;[15]

---

12 *South China Morning Post,* 9 July 1995.
13 Section 27.
14 Section 28.
15 Section 29.

(d) destroying any postal packet or anything contained therein;[16]

(e) sending by post any "prohibited articles" including "any obscene, immoral, indecent, offensive or libellous writing, picture or other thing", or "any seditious publication within the meaning of any enactment relating to sedition".[17]

2.27 These offences are accompanied by extremely wide powers of interception.

Power of Postmaster General to open postal packets

(a) Power to open postal packets without warrant

2.28 The Postmaster General may open and delay any postal packet under section 12 of the Post Office Ordinance without any warrant if he has reason to believe that the packet -

- has been posted in contravention of the Post Office Ordinance;
- contains anything which may not legally be sent by post;
- contains anything with respect to which or by means of which any offence has been or is being committed or attempted; or
- contains dutiable article.

2.29 In addition, an officer of the Post Office may open any postal packet upon which proper postage has not been paid or which cannot be delivered.[18]

2.30 We shall examine in chapter 5 whether section 12 provides sufficient safeguards against undue interference with privacy.

(b) Power to open postal packets with warrant

2.31 The provision addressing warrants is section 13 of the Post Office Ordinance:

> *"(1) It shall be lawful for the Chief Secretary to grant a warrant authorizing the Postmaster General, or authorizing any or all the officer of the Post Office, to open and delay any specified postal packet or all postal packets of any specified class or all postal packets whatsoever.*
>
> *(2) It shall be lawful for the Postmaster General to delay any postal packet for such time as may reasonably be*

---

16 Section 26.
17 Section 32.
18 Section 10.

necessary for the purpose of obtaining a warrant under this section."

2.32 This is in even broader terms than its counterpart, section 33 of the Telecommunication Ordinance. Section 13 lacks any reference to a reasonable belief or a "public interest" requirement, and the authorising officer is the Chief Secretary rather than the Governor.

2.33 It follows that the Post Office Ordinance purports to sanction the interception of mail for whatever reason. Its likely incompatibility with article 17 of the ICCPR and article 30 of the Basic Law will become more apparent with Chapter 3's discussion of the *Klass* and *Malone* cases.[19]

Protection of personal data

2.34 While anti-hacking provisions target the *intruder*, the Personal Data (Privacy) Ordinance (Cap. 486) requires *users* of personal data not to do anything that contravenes a data protection principle set out in the schedule to the Ordinance.

2.35 Data protection principle 1 provides that:

(a) personal data should not be collected unless the data are collected for a lawful purpose directly related to a function or activity of the data user; and

(b) personal data should be collected by means which are lawful and fair.

2.36 For the purposes of safeguarding the storage and transmission of personal data, data protection principle 4 provides that all practicable steps should be taken to ensure that personal data held by a data user are protected against unauthorized or accidental access, processing, erasure or other use. "Data user" in this context may be the person storing or transmitting the data.[20]

2.37 Press reports indicate that data security has yet to be accorded sufficient importance in Hong Kong. A team from the Royal Melbourne Institute of Technology visiting in February 1992 concluded that many of Hong Kong's large companies were lax in protecting their confidential data. They observed a common misconception that computer risks were limited to breakdowns and viruses.

2.38 With the enactment of the Personal Data (Privacy) Ordinance (Cap. 486) in August 1995, both individuals and public and private sector

---

[19] Section 13 can be repealed if our proposals on the warrant system are adopted. See chapter 6 below.

[20] Section 2(1) & (12).

organisations should become more aware of their rights as data subjects and their obligations as data users.

2.39 On appointment as the Privacy Commissioner for Personal Data on 1 August 1996, Mr. Stephen Lau Ka-men declared that his immediate tasks included :

(a) the launching of a major promotion and public education campaign to heighten the awareness of the importance and provisions of the Ordinance;

(b) the establishment of an enquiries and complaints system relating to the protection of personal data; and

(c) liaison with major data users in both private and public sectors.

2.40 Most of the core provisions of the Ordinance will come into operation on 20 December 1996.[21] We believe that the implementation of the Ordinance will better protect individual privacy and will improve Hong Kong's competitiveness as an international trading and financial centre.

[21] Personal Data (Privacy) Ordinance (Cap 486) (Commencement) (No 2) Notice 1996, LN 514 of 1996. The provisions on matching procedures and transfer of personal data will be implemented in June 1997: *Hong Kong Standard*, 9 November 1996.

Chapter 3

The legal protection of privacy of communications

Summary

3.1 We explained in the Introduction that there is an increasing need for privacy of communications in society. This chapter examines the legal protection of privacy of communications afforded by the common law and human rights jurisprudence. It will be seen that the common law provides no effective protection to the privacy of communications. However, the jurisprudence of the European Court of Human Rights provides a comprehensive framework of protection. This is relevant to Hong Kong for the following reasons:

- *The ICCPR has been extended to Hong Kong by the United Kingdom, and the European jurisprudence is relevant to the ambit of article 17 of that treaty.*
- *The provisions of article 17 are replicated in article 14 of the Hong Kong Bill of Rights.*
- *The Basic Law guarantees that the provisions of the ICCPR will remain in force and will be implemented through the laws of the Hong Kong Special Administrative Region.*

We conclude that the present provisions of the Telecommunication Ordinance and Post Office Ordinance do not accord with the requirements of article 17 of the ICCPR.

The common law protection of privacy of communications

3.2 There is no right of privacy at common law.[1] Such protection for the privacy of individuals as there is at common law is inadequate in safeguarding the privacy of communications.[2] This will become obvious as we consider below the following causes of action in civil law:

---

1 *Kaye v Robertson* [1991] FSR 62.

2 Cf *Report of the Committee on Privacy* (London, Cmnd 5012, 1972) ("the Younger Report"), Appendix I; *Infringement of Privacy: Consultation Paper* (The Scottish Office, Lord Chancellor's Department, 1993), chapter 4.

(a) Trespass to land;
(b) Nuisance;
(c) Breach of confidence; and
(d) Defamation.

Trespass to land

3.3 A civil action will lie in the tort of trespass to land when, without justification, the defendant enters on the plaintiff's land, remains on such land or places any object upon it. This action protects a person's property and his enjoyment of it, rather than his privacy as such. This action cannot protect an individual's communications if the interception is effected from outside his property. Indeed, interception of telecommunications and mail seldom involves trespass to land. Even if it does, a person who is not entitled to exclusive possession of the land, such as a visitor or a member of the owner's family, would not be able to sue the intruder for trespass.

Nuisance

3.4 A plaintiff will have a cause of action in private nuisance if the defendant's act prejudiced or disturbed his enjoyment of land. This action only protects the person in possession of the land injuriously affected. Persons who do not have exclusive possession of the land cannot maintain an action for nuisance. But even if the individual has exclusive possession, it is doubtful whether he could sue the intruder for nuisance if the interception had no physical effects on his land. In relation to interception of communications, the intruder has no intention of disturbing the target's enjoyment of his land. On the contrary, the intruder hopes that the target's behaviour will remain unchanged during the course of the interception.

Breach of confidence

3.5 There are three elements of a successful action for breach of confidence:

- the information must have the necessary quality of confidence about it;
- that information must have been imparted in circumstances importing an obligation of confidence; and
- there must be an unauthorised use of that information to the detriment of the party communicating it.

3.6 The aggrieved party cannot rely on this action if no confidential information is communicated. Whereas the right of maintaining an action for breach of confidence is based on an obligation of confidence owed to another, a general right of privacy in respect of information arises from the

personal nature of the information, regardless of any relationship or duty of confidence. Even if confidential information is involved and the confidant is under an obligation to maintain confidence, the aggrieved party has no remedy for breach of confidence if the information is not used or disclosed by the confidant. The action also suffers from the limitation that it is only the person to whom the duty of confidence is owed who is entitled to bring an action. If A imparts information about B in confidence to C, B cannot maintain an action for breach of confidence if C discloses the information.

Defamation

3.7 This tort is relevant only if there was a *publication* of a false and defamatory statement concerning another person without lawful justification. It cannot help an aggrieved individual where an interception was not followed by any publication or the publication does not tend to injure his reputation. Furthermore, he does not have a cause of action if the statement is true, even though the statement may relate to his private life. It is clear that the action aims at the discloser and not the intruder and it protects an individual's reputation rather than his privacy.

Malone v Metropolitan Police Commissioner (No. 2) : A review of the common law

3.8 The common law position regarding telephone interceptions was comprehensively reviewed by the Chancery Division decision of *Malone*[3]. The matter was subsequently taken to the European Court of Human Rights and the court's ruling provided the impetus for the United Kingdom Interception of Communications Act 1985.[4]

3.9 Malone was charged with handling stolen goods. During the trial, a police officer admitted that Malone's phone had been tapped. Details of a telephone conversation to which Malone had been a party were found to be contained in a police notebook. Counsel for the prosecution then accepted that this conversation had been intercepted on the authority of a warrant issued by the Secretary of State. Malone subsequently instituted civil proceedings in relation to the tapping of his telephone. It was not claimed that the tap entailed any trespass on his premises. The issue was whether telephone tapping in aid of the police was illegal. Expressly excluded from consideration was "tapping that involved electronic devices which make wireless transmission", as was any process whereby anyone trespasses onto private premises to affix tapping devices.

3.10 Malone put forward the following arguments:

---

3 [1979] Ch 344.

4 See paragraphs 3.29 *et seq.*

(a) ***Right to property in one's telephone conversation*** It was contended that a person had rights of property in his words as transmitted by the electrical impulses of the telephone system, and so the tapping constituted an interference with his property rights. This was rejected by the court as lacking reality.

(b) ***Eavesdropping*** Whilst it was conceded that there was no general right to privacy at common law, it was argued that there was a right to hold a telephone conversation in the privacy of one's home without molestation. The principal basis of this contention was the common law offence of eavesdropping, an offence constituted by listening just outside a house with the object of spreading slanderous and mischievous tales.[5] That offence had, however, been repealed by the Criminal Law Act 1967 (though not in Hong Kong). The judge in any case concluded that telephone tapping was outside the mischief of the doctrine.

(c) ***Confidentiality*** The court held that:

> "*The application of the doctrine of confidentiality to the tapping of private telephone lines is that in using a telephone a person is likely to do it in the belief that it is probable (though by no means certain) that his words will be heard only by the person he is speaking to."*[6]
>
> *"It seems to me that a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of communication ... [T]he Younger Report referred to users of the telephone being aware that there were several well-understood possibilities of being overheard, and stated that a realistic person would not rely on the telephone system to protect the confidence of what he says."*[7]

3.11 The jurisprudence of the European Court has come to a different conclusion and this is examined below.

3.12 In its report entitled *Breach of Confidence,* the English Law Commission referred to the finding of the English court, commenting: "We do not think that in a civilised society a law abiding citizen using the telephone should have to expect that it may be tapped."[8] Their recommendation that the duty of confidence be extended to apply to surreptitiously obtained information will be examined in our report on surveillance.

---

5 The offence of eavesdropping is a common nuisance. It may be committed by "listen[ing] under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales" : J W C Turner, *Russell on Crime* (London: Stevens and Sons, 12th ed, 1964), vol 2, page 1397.

6 *Ibid,* at 360.

7 *Ibid,* at 376.

8 Law Commission Report No 110, at paragraph 6.35.

3.13 The Law Commission's rejection of the notion that awareness of the possibility of surveillance should be treated as signifying acquiescence is echoed by many commentators. As one puts it:

> *"Free conversation is often characterised by exaggeration, obscenity, agreeable falsehoods, and to the expression of antisocial desires or views not intended to be taken seriously. The unedited quality of conversation is essential if it is to preserve its intimate, personal and informal character."*[9]

3.14 The judge in *Malone* concluded his judgment by reiterating that his decision was confined solely to tapping pursuant to a warrant for police investigation.

European Court decisions on interception of communications

3.15 Article 17 of the International Covenant on Civil and Political Rights ("ICCPR") provides in part that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". That provision is replicated as section 8, article 14 of the Hong Kong Bill of Rights Ordinance. In view of the lack of relevant jurisprudence under the ICCPR, it is necessary to consider the decisions of the European Court of Human Rights which interpret the similar provisions of article 8 of the European Convention on Human Rights.

3.16 The interception of communications has been a fertile source of complaints to the European Court. The decisions apply the same principles to both written correspondence and telecommunications. The two most important decisions are *Klass*[10] and *Malone*[11]. In *Klass,* telephone tapping was conducted pursuant to detailed legislation. In the later decision of *Malone* it was conducted in the absence of a comprehensive legislative scheme. Although the facts of both cases involved conventional "taps" of analogue telephones, the principles articulated are sufficiently general to encompass all the modern forms of interception of telecommunications discussed above. Nor are the decisions restricted to the interception of telecommunications. The principles set out also apply to the interception of written correspondence, and arguably to other forms of surveillance.

3.17 Before we give a detailed account of the arguments leading to the decisions in *Malone* and *Klass*, we set out below the main points highlighted by the European Court in these two cases which are relevant for our purposes:

(a) The phrase "in accordance with the law" in article 8 of the European Convention does not refer merely to the domestic law, whether written

---

9 L B Schwarz, *"On Current Proposals to Legalise Wiretapping"* (1954) 103 *Univ. of Pa. Law Rev.* 157, 162, quoted in Wacks, *op cit,* at 247.

10 (1978) 2 EHRR 214.

11 (1984) 7 EHRR 14.

or unwritten, but also relates to the quality of the law, meaning that it must be compatible with the rule of law.

(b) The phrase thus implies that there must be a measure of legal protection in domestic law against arbitrary interference by the executive with the individual's right to respect for his private life and correspondence.

(c) The law must indicate with sufficient clarity the scope of any discretion conferred on the public authorities and the manner of its exercise so as to give the individual adequate protection against arbitrary interference.

(d) The rule of law implies that any interference by the executive with an individual's rights should be subject to effective control which should normally be assured by the judiciary, at the least in the last resort. In the field of surveillance where abuse is potentially so easy in individual cases, it is desirable to entrust supervisory control to a judge in principle.

3.18 The remaining paragraphs examine the three European Court decisions on interception of communications, namely, *Klass*, *Huvig* and *Malone*. The implications of these decisions for the Telecommunication Ordinance and the Post Office Ordinance are explained at the end of this chapter.

Klass v Federal Republic of Germany[12]

3.19 In *Klass* the Court considered the adequacy of a comprehensive statutory regime regulating interceptions. The applicants in this case, five German lawyers, challenged the statutory regime as contravening article 8 of the European Convention. In particular, they challenged the lack of a requirement that the individual be invariably notified following the cessation of surveillance. The government objected that the applicants seeking the review of the legislation were not claiming to have established specific violations but only the purely hypothetical possibility of being subject to surveillance. The Court rejected this on the basis that the contested legislation instituted a system of surveillance exposing all residents to the possibility of being unwittingly monitored. It was the possibility rather than the demonstrated fact of surveillance that was relevant. The question of whether the applicants were victims of a violation therefore turned on the compatibility of the surveillance law with the European Convention, and not on whether concrete measures had been applied to them.[13]

3.20 A related point is that the mischief of interference with a person's private life is quite independent of whether information relating to that person's "private life" was successfully obtained. This would accord with Wacks' position that the essential objection to surveillance is independent of

---

12 (1978) 2 EHRR 214.

13 Cf D Lyon, *The Electronic Eye: The Rise of Surveillance Society,* (Minneapolis, 1994), at 60.

the quality of information thereby obtained: it is that there has been an intentional interference with the individual's interest in seclusion or solitude.[14]

3.21 The German Basic Law secures secrecy of the mail, post and telecommunications. The issue before the court in *Klass* was therefore whether interference was justified under article 8(2) of the European Convention as being "in accordance with the law" and necessary in a democratic society "in the interests of national security ... or for the prevention of disorder or crime." The Court accepted the legitimacy of legislation providing for interceptions for these public interest purposes. It took judicial notice of the overt terrorism threat existing at the time. The issue was not the need for such provisions, but whether they contained sufficient safeguards against abuse, thus checking a slide towards totalitarianism:

> "*The Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court ... affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*
>
> *The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law."*[15]

3.22 Restrictions were exhaustively provided for in a statute enacted pursuant thereto. Interceptions of mail and telecommunications required fulfilment of the following conditions:

1) Applications must be made in writing by the departmental head or his deputy, giving reasons. There must be a factual basis for suspecting a person of planning, committing, or having committed certain criminal or subversive acts. Surveillance may cover only the specific suspect or his presumed contact persons. "Exploratory" or general surveillance is therefore not permitted.

2) Other investigatory methods would be ineffective or considerably more difficult.

3) The interception is supervised by a judicial officer who transmits to the investigative authorities only information relevant to the

---

14 See Introduction above.

15 (1978) 2 EHRR 214, paras 49 and 50.

inquiry and destroys the residue. The transmitted information must itself be destroyed when no longer required, nor may it be used for any other purpose.

4) The interception must be immediately discontinued upon the cessation of these requirements and the individual concerned notified as soon as this can be done without jeopardising the purpose of the interception. The individual may then have the legality of the interception reviewed by the administrative court and claim damages in a civil court if he has been prejudiced.

5) The relevant minister must report monthly to an independent Commission comprising a judge and two assessors on the measures ordered. At its own initiative, or upon application by a person believing himself to be subject to surveillance, the Commission may order that the measures be terminated. Every six months the Minister must also report to a Board consisting of five parliamentarians.

3.23 Only two aspects of this scheme were challenged by the applicants. One related to the lack of a requirement that the subject of surveillance be *invariably* notified upon its cessation. The Court held that this was not inherently incompatible with article 8, provided that the person concerned was informed after the termination of the surveillance measures as soon as notification could be made without jeopardising the purpose of those measures.

3.24 The other criticism made by the applicants related to the fact that the system of controls were administrative rather than judicial. The Court agreed that effective controls should normally be assured by the judiciary, at least in the last resort, as judicial control offered the best guarantee of independence, impartiality and a proper procedure. The Court noted that only in exceptional circumstances could the individual apply to the Commission and thereafter to the Constitutional Court. The latter was empowered to seek information and documents. The general position, however, was that judicial controls were excluded. Instead, they were replaced by the administrative system of controls described above. The Court held that, while it was in principle desirable to entrust supervisory control to a judge, the measures adopted were sufficient. The Court was satisfied that the supervisory bodies were independent of the authorities carrying out the surveillance, and vested with sufficient powers and competence to exercise an effective and continuous control. Also relevant was their balanced membership. Accordingly, the court was satisfied that "the two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling."

Huvig v France[16]

3.25 In this case, the European Court examined the position under French law, whereby telephone tapping is carried out by police under a warrant issued by an investigating judge. Before Huvig had been charged with tax evasion, his telephone calls were intercepted over a two day period. No evidence was obtained from the tappings. At the subsequent trial he disputed the legality of the tapping. The Appeal Court upheld the legality of the tapping, and Huvig appealed to the European Court.

3.26 The statutory provisions governing the matter were general in nature, conferring an investigating judge with a discretion to authorise any "investigative measure" he deems necessary or useful. There must be a ground for suspicion and tapping may not be authorised on the off-chance of discovering crime. This power was unaffected by a provision in the criminal code making it an offence to intercept communications.

3.27 The Court had no difficulty in finding that the tapping constituted an interference with Huvig's privacy. It then considered whether that interference was "in accordance with law". The Court held that not only statutory but also case law constituted "law" in this context. However, neither source of law addressed the following matters:

- the categories of persons liable to interceptions;
- the offences susceptible to interceptions;
- the duration of interception warrants;
- the specification of procedures regarding summarisation of intercepted conversations; and
- the erasure or destruction of the tapes.

3.28 The Court upheld the applicant's claim that the interception was not "in accordance with the law." This was because the law "does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."

Malone v United Kingdom[17]

3.29 *Malone* is the genesis of the United Kingdom Interception of Communications Act 1985. In that case, the European Court of Human Rights did not find wanting the administrative arrangements governing the interception of communications. Rather, the deficiency related to their not being given clear legal effect. Sir Robert Megarry held that Malone had no remedy under English law for the reasons set out above, but added that "it is plain that telephone tapping is a subject which cries out for legislation". Malone then took the matter to the European Court.

---

16 (1990) 12 EHRR 528.
17 (1984) 7 EHRR 14.

3.30 ***Scope of the decision*** The Court explicitly noted at the outset that the scope of the case did not extend to interception of communications generally, but dealt only with interceptions effected by or on behalf of the police (not Customs or the Security Service) for the investigation of crime.

3.31 The first issue for the Court related to the legitimacy of the interception of communications on behalf of the police. "Interception" was defined as "the obtaining of information about the contents of a communication by post or telephone without the consent of the parties involved." The Court held that telephone conversations were covered by the notions of "private life" and "correspondence" within the meaning of article 8. The admitted interception of the call adverted to in the trial accordingly constituted "interference" with the exercise of the right to privacy guaranteed under the provision. Malone also claimed that both his mail had been opened and his telephone tapped for a number of years. However, the Government declined to disclose whether this was so, claiming that such disclosure would frustrate the purpose of such interceptions and could jeopardise sources of information. For its part, the Court did not consider it necessary to inquire further into Malone's claims in upholding his claim as:

> *"the existence in England and Wales of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an 'interference ... with the exercise' of the applicant's rights under Article 8, apart from any measures actually taken against him."*[18]

3.32 This follows the approach taken in *Klass* discussed above where the Court noted that State-instituted surveillance measures are necessarily conducted without the subject's knowledge. To require that an individual prove that such measures were in fact applied to him would effectively reduce the right to privacy to a nullity. It was therefore sufficient that there be evidence of a system of surveillance.

3.33 The Court then turned to consider whether the interference was justified as "in accordance with the law" under article 8. "In accordance with the law" encompassed both written and unwritten law and the interference must have some basis in domestic law. The Court accepted that such interference was lawful in England. However, compliance with domestic law was not in itself sufficient. The quality of the law was also relevant:

> *"The phrase ['in accordance with the law'] thus implies ... that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by [article 8(1)] ... the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially*

[18] (1984) 7 EHRR 14, para 64.

dangerous interference with the right to respect for private life and correspondence ... ."[19]

"[In Silver v United Kingdom,] the Court held that 'a law which confers a discretion must indicate the scope of that discretion', although the detailed procedure and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. The degree of precision required of the 'law' in this connection will depend upon the particular subject matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or by the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered law. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."[20]

3.34 The Court then applied these criteria to the applicable domestic laws invoked as authorising the interception. It accepted that there was a long established practice of intercepting postal and telephone communications pursuant to a warrant issued by the Home Secretary. An application for a warrant must be put forward by a senior police officer in writing and be submitted in the first instance to a senior civil servant. The application must contain a statement of the purpose for which interception was requested, and the facts supporting the request. Three conditions needed to be satisfied:

a) The offence must be "really serious". The Court noted that the scope of this concept had been varied from time to time by the executive.

b) Normal methods of investigation must have been tried and failed or must, from the nature of things, be unlikely to succeed.

c) There must be good reason to think that an interception would be likely to lead to an arrest and conviction.

3.35 The issue of the warrant in accordance with these criteria would then be personally considered by the Home Secretary. Upon issue of the warrant, relevant details would be specified, including the name and address of the recipient of the mail or the telephone number to be monitored. A time limit of initially not more than two months was stipulated. Reviews were conducted monthly. Separate warrants were required for the interception of both mail and telephone calls. Records were kept of all warrants issued.

---

19 (1984) 7 EHRR 14, para 67.

20 (1984) 7 EHRR 14, para 68.

Application procedures were detailed in a circular to police. On issue of the warrant, the interception was effected by the telecommunications authority taping the call or copying the letter and providing it to the police. The police noted or transcribed only such parts of the correspondence or conversation as were relevant to the investigation. The tape would then be returned and erased, usually within one week. The notes of transcriptions of intercepted communications would be retained until they were no longer required for the purposes of investigation, and then destroyed. The information was used solely for investigative purposes and was not tendered in evidence, nor disclosed to others. The individual whose communications had been intercepted was not informed of the fact, even when the surveillance and the related investigation had been terminated.

3.36 The Court was able to conclude that, although there was no overall statutory code governing the matter, "detailed procedures concerning interception of communications on behalf of the police in England and Wales do exist." Furthermore, the public had been informed of the applicable arrangements. Illegal interceptions were subject to criminal and civil proceedings. However, the legal basis of the practice, regulated in part by assorted statutory provisions, was "somewhat obscure and open to different interpretations." The Post Office statutes recognised, rather than conferred, authority to intercept communications and it was unclear whether a valid warrant was required to authorise an interception. Crucially, it was also unclear what, if any, statutory restrictions applied to the purposes for which, and the manner in which, interceptions of communications might be authorised by the Home Secretary. The Government argued that the relevant provision of the Post Office Act defined and restricted the power to intercept by reference to the procedures described in the paragraph above. But there was also an argument that the statutory provisions did not incorporate those procedures, or any of them, and that no clear legal restrictions controlled the issue of warrants. Indeed, the Home Secretary's discretion was arguably unfettered. The Court accordingly concluded from the evidence that:

> *"It cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect ... the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."*[21]

3.37 The Court held that the minimum degree of legal protection to which citizens were entitled under the rule of law was lacking. Although the Court agreed that the existence of some law granting powers of interception of communications to aid the police in the investigation and detection of crime may be necessary in a democratic society, it opined that:

---

[21] (1984) 7 EHRR 14, para 79.

> *"the existence of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole. This being so, the resultant interference can only be regarded as 'necessary in a democratic society' if the particular system of secret surveillance adopted contains adequate guarantees against abuse."*[22]

3.38 ***Metering*** Malone not only challenged the legitimacy of intercepting telephone conversations, but also the process of "metering" such calls. This process employs a device which registers the numbers dialled on a particular telephone and the time and duration of each call. The telecommunications authority would provide its records at the request of the police if the information was essential to the investigation of serious crime and could not be obtained from other sources.

3.39 The Court noted that the metering process makes use only of signals sent to the provider of the telephone service for the legitimate purposes of billing and the investigation of complaints. No monitoring or interception of the contents of telephone calls was involved. But the Court rejected the Government's contention that the use of metering data may not therefore interfere with privacy rights. It held that metering records provide data, particularly the numbers dialled, "which is an integral element in the communication made by telephone" and that the subsequent disclosure of the data to the police without the subscriber's consent amounted to an interference with the right to privacy. There was no conclusive evidence that Malone's calls had been metered, the Government having denied doing so. However, there was evidence of a practice whereby upon request the Post Office would provide its records to the police. The Court held that it was this very practice which interfered with Malone's privacy rights, quite apart from any concrete measures specifically aimed at him.

3.40 The remaining issue was whether such interference was "in accordance with the law". The Post Office practice had been made public in answers to parliamentary questions. Apart from the simple lack of a statutory prohibition, no legal rules were adduced concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. The Court therefore concluded that, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question was not "in accordance with the law" within the meaning of article 8(2).

3.41 We recommend below that a warrant be required to authorise any interception of communications falling within the scope of the proposed offence prohibiting such activities. As the release of metering data by the telecommunications carrier to the police does not in itself involve any interception of communications, the police do not need a warrant before they can gain access to such data. However, insofar as the metering data relate

---

[22] (1984) 7 EHRR 14, para 81.

directly or indirectly to an individual, the collection and use of such data are subject to the provisions of the Personal Data (Privacy) Ordinance.

3.42 ***The sequel to Malone: The Interception of Communications Act*** In February 1985, six months after the European Court handed down its decision in *Malone*, the Home Office released a White Paper proposing the introduction of legislation to provide a clear statutory framework governing the interception of communications "on public systems" (a limitation not adverted to in *Malone).*[23] Subsequently, the Interception of Communications Act 1985 was enacted. The legislation is open to criticism on a number of counts, some of which are discussed in the next chapter. Its relevance to our present study, however, is that it addresses many of the matters not covered by either the Telecommunication Ordinance or the Post Office Ordinance in Hong Kong.

Implications for the Telecommunication Ordinance and the Post Office Ordinance

3.43 The principles underlying the decisions of the European Court are consistent with the views expressed by the United Nations Human Rights Committee referred to in the Introduction above.[24] They are in line with the object of article 17 of the ICCPR and ought to be taken into account in implementing that article.

3.44 In light of the European Court decisions explained above, section 33 of the Telecommunication Ordinance (Cap. 106) and section 13 of the Post Office Ordinance (Cap. 98) can be said to suffer the following drawbacks:

(a) The provisions do not specify the grounds on which an interception may be carried out. While section 33 of the Telecommunication Ordinance provides that the Governor or an authorised officer may order the interception of telecommunications "whenever he considers that the public interest so requires", section 13 of the Post Office Ordinance goes even further and omits the public interest test. In other words, the Chief Secretary has unfettered discretion and may grant a warrant authorising interception of mail without giving any reason.

(b) Neither the Governor (or an officer authorised by him) nor the Chief Secretary is required to have any grounds for suspicion when authorising an interception. An officer who applies for an order needs not swear an affidavit deposing as to the facts upon which he holds the opinion that an interception is necessary.

---

23 *The Interception of Communication in the United Kingdom* (Cmnd 9438, 1985).

24 Paragraph 26 in the Introduction.

(c) The authorising officer is not required to be satisfied that the information sought by the applicant cannot reasonably be obtained by other less intrusive means.

(d) The provisions do not impose any restrictions as to the duration of an interception authorised by an order or warrant. In theory, an order or warrant may be indefinite in length.

(e) The provisions make no requirements on the content of an order. There is no guarantee that the scope of the measures authorised by an order is narrowly defined. In fact there is nothing in the two ordinances which prohibits the granting of a blanket authorisation for the interception of telecommunications or mail.

(f) The making of orders or the granting of warrants authorising interception of communications are not monitored by an independent body on a regular basis.

(g) The officer making the order or warrant is not accountable to the public at large. He or she is not required to report on the granting of warrants and the measures taken pursuant to a warrant.

(h) The provisions do not provide for any means by which the legality of an interception can be reviewed by a judicial or administrative body.

(i) The provisions do not provide for any judicial or administrative remedies for an individual who suffers damage by reason of an interception which had been improperly authorised.

3.45 Neither ordinance can therefore be said to "be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which" interceptions may be authorised. We conclude that the two ordinances do not provide sufficient protection against unlawful or arbitrary interference with the individual's right to privacy and freedom of communication.

3.46 It is clear that legislation must be in place to regulate the interception of communications. The regulatory framework to be provided by law must contain adequate safeguards against abuse. We examine in the remainder of this report proposals which will satisfy the requirements spelt out in the jurisprudence examined above.

Chapter 4

Interception of communications: legal issues

Summary

4.1 We explain in this chapter why criminal sanctions are necessary to protect communications from interception. We then identify the mischief to be addressed in regulating the interception of communications. We conclude that :

- *Communications should be safeguarded from interception or interference while they are in the course of transmission.*
- *The protection should cover all communications transmitted by a communications system, whether the system is private or public.*
- *All unauthorised interceptions should be prohibited, whether they come from the public or the private sector.*

4.2 We agree that the following types of interception may be lawfully carried out:

- *interception with the consent of one party to the communication;*
- *interception to ensure compliance with licensing conditions; and*
- *interception by telecommunication carriers for operational purposes.*

4.3 We take the view that employee communications sent to the place of employment should be presumed work-related unless words like "private" or "personal" are marked on the cover.

Recommendations

4.4 It should be an offence intentionally to intercept or interfere with -

(a) a telecommunication;
(b) a sealed postal packet; or

(c) a transmission by radio on frequencies which are not licensed for `broadcast,

while the telecommunication, postal packet or radio transmission is in the course of transmission.

4.5 "Interference" for the purposes of the proposed offence should include destruction, corruption or diversion.

4.6 Anyone who contravenes the proposed offence should be liable to a fine or a term of imprisonment not exceeding 5 years or both.

4.7 A person should not be guilty of the proposed offence if

(a) one of the parties to the communication has consented to the interception;

(b) the communication is intercepted for purposes connected with the prevention or detection of radio interference or for ensuring compliance with a licence issued under the Telecommunication Ordinance; or

(c) the communication is intercepted for purposes connected with the provision of telecommunication service or with the enforcement of any enactment relating to the use of that service.

4.8 The Telecommunications Authority should specify in the licences granted under the Telecommunication Ordinance the circumstances under which and the extent to which interceptions for operational purposes may be carried out. Such terms and conditions should also be made available to the public for inspection.

The need for criminal sanctions

4.9 There are a number of reasons why criminal sanctions are necessary to protect communications from interception or interference:

(a) Interception of communications is a serious intrusion upon individual privacy which warrants the use of criminal sanctions. Regulating interceptions by means of the criminal law would ensure that police assistance would be given to the victim in identifying the source of intrusion.

(b) The victim has no remedy in civil law. Civil actions like trespass to land and nuisance which provide some protection against intrusion into private premises are irrelevant where the interception of communications was effected without unauthorised entry into private premises. Further, it is only when *confidential* information obtained

through interception is *disclosed* that the victim may have a remedy in breach of confidence.[1]

(c) It is a requirement of the ICCPR and the Hong Kong Bill of Rights that everyone has the right to the protection of the law against arbitrary or unlawful interference with their privacy and correspondence.[2] The Basic Law of the Hong Kong Special Administrative Region also guarantees that the freedom and privacy of communications of Hong Kong residents will be protected by law.[3]

(d) It accords with the reasonable expectations of both parties to the communication that any interference with their communications should be prohibited unless authorised by an authority designated under the law.

(e) There is an increasing need for privacy and security of telecommunications. The increased amount of personal information available on-line or generated by using the phone is a major factor.

(f) The use of criminal sanctions to protect communications is not without precedent in Hong Kong. The following are some examples:

- Section 27 of the Telecommunication Ordinance (Cap. 106) prohibits interference with a telecommunication installation with intent to intercept the contents of a message.

- Regulation 9(1) of the Telecommunication (Control of Interference) Regulations (Cap. 106, sub. leg. A) prohibits the use of any apparatus for the purpose of interfering with the working of a telecommunication apparatus.

- Section 27 of the Post Office Ordinance provides that no person shall open or delay the delivery of any postal packet which is in the course of transmission.

(g) As explained in Chapter 2 above, the effectiveness of the provisions of the Telecommunication Ordinance and the Telecommunication Regulations in safeguarding the privacy of telecommunications is seriously impaired by including interference with a telecommunication installation or apparatus as an element of the offence. A wider offence targeting specifically interference with *communications,* with no reference to a telecommunication installation or apparatus, would provide a more effective remedy.

4.10 In light of the foregoing arguments, we conclude that criminal sanctions are necessary to protect communications from interception.

---

1 See paragraphs 3.2 - 3.14 above.

2 See also the opinion of the UN Human Rights Committee quoted in the Introduction.

3 Article 30. See paragraphs 24 to 32 in the Introduction.

Experience in other jurisdictions

4.11 The Hong Kong Journalists Association and the Hong Kong News Executives Association commented that the United States and many other common law jurisdictions choose to deal with the issue of privacy by the law of tort. This is inaccurate as far as the interception of communications is concerned. Several jurisdictions, including common law jurisdictions, have legislation regulating interception of communications. Although the scope of protection afforded by such legislation varies, all the statutes apply criminal sanctions to safeguard the privacy interests of individuals in one way or another. The following paragraphs briefly summarise the position in Australia, Canada, Germany, New Zealand, South Africa, United Kingdom, and the United States:

(a) *Australia*

The Telecommunications (Interception) Act 1979 of the Commonwealth prohibits the interception of communications passing over a telecommunications system except where authorised in special circumstances. Anyone who intercepts a telecommunication commits an offence under section 7(1) and is liable to imprisonment for a period not exceeding 2 years.[4]

The 1979 Act is supplemented by listening devices legislation at the state level. The purpose of this legislation is to prohibit the use of a listening device to record or listen to any private conversation to which the person using the device is not a party.

(b) *Canada*

Section 184 of the Criminal Code[5] makes it an offence, subject to a number of exceptions, to intercept private communications by means of any electro-magnetic, acoustic, mechanical or other device, and provides that the offender is liable to imprisonment for a term not exceeding 5 years.

(c) *Federal Republic of Germany*

Article 10 of the Basic Law of the Federal Republic of Germany declares the privacy of correspondence, posts and telecommunications to be inviolable. Restrictions may only be ordered pursuant to a law. The Act on Restriction of the Secrecy of Mail, Posts and Telecommunications was enacted to implement article 10.[6]

---

4 Section 105.

5 RSC 1970, c. C-34, as amended.

6 The Act was enacted on 13 August 1968. It was amended by another Act on 8 June 1989.

(d) *New Zealand*

Section 216B of the Crimes Act 1961 provides that, subject to certain exceptions, a person who intentionally intercepts a private communication by means of a listening device is liable to imprisonment for a term not exceeding 2 years.[7]

(e) *Republic of South Africa*

Section 2 of the Interception and Monitoring Prohibition Act 1992 provides that no person shall:

(i) intentionally intercept a communication which is transmitted by telephone or over a telecommunications line; or

(ii) intentionally monitor a conversation by means of a monitoring device so as to gather confidential information.

Any person who contravenes this provision is liable to imprisonment for 2 years.

(f) *United Kingdom*

Under section 1 of the Interception of Communications Act 1985, a person who intentionally intercepts a communication in the course of its transmission by post or by means of a public telecommunication system is guilty of an offence and is liable to imprisonment for 2 years.

(g) *United States*

Section 2511 of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) ("the Wiretap Act") provides that except as otherwise provided in the Act, any person who:

(i) intentionally intercepts any wire, oral or electronic communication; or

(ii) intentionally uses any electronic, mechanical or other device to intercept any oral communication when one of the specified conditions is met,

is liable to imprisonment for 5 years.

---

[7] For the position in New Zealand, see Longworth Associates, *Telecommunications and Privacy Issues* (New Zealand, Ministry of Commerce, Communications Division, 1992).

"Interception of" or "interference with" communications

4.12 Having concluded that it is necessary for interception of communications to be regulated by law, we now consider the mischief to be regulated, and whether this is satisfactorily defined by the phrase "*interception* of" or "*interference* with" communications.

"Interception"

4.13 The legislation of the major common law jurisdictions, including Australia, the United Kingdom, the United States and New Zealand, all focus on "interception."

4.14 "Interception" is not defined in the United Kingdom Interception of Communications Act 1985. The New Shorter Oxford English Dictionary defines "intercept" as:

> *"Put an end to, check, (an action, effect, etc.). ... Prevent, hinder, (a person or thing). ... Obstruct so as to prevent from continuing to a destination; stop in the course of a journey; obtain covertly (a message etc. meant for another); ..."*

4.15 We believe that this meaning adequately describes the conduct which ought to be proscribed by law. In the context of interception of communications, we agree that "intercept" basically means the acquisition of the contents of a communication or the prevention, hindrance or obstruction of the transmission of a communication. We note that this view accords with the definitions of "intercept" in the provisions of other common law jurisdictions.[8]

4.16 Tracing the source of a communication does not normally involve an interception of communications because it is possible to identify the source without knowing the contents of a communication. However, the release of data relating to the source by a service provider is governed by the provisions of the Personal Data (Privacy) Ordinance (Cap. 486).[9]

Interception "in the course of transmission"

4.17 Black's Law Dictionary makes the point that "'interception' does not ordinarily connote the obtaining of what is to be sent before, or at the

---

[8] Section 2510 of the United States Wiretap Act provides: *"'Intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."* In Canada, section 183 of the Criminal Code provides that "intercept" means "*listen to, record or acquire a communication or acquire the substance, meaning or purport thereof*." As for New Zealand, section 216A of the Crimes Act 1961 (see Crimes Amendment Act 1979, section 2) provides that "'*[intercept]', in relation to a private communication, includes hear, listen to, record, monitor, or acquire the communication while it is taking place*".

[9] Cf paragraph 3.41 above.

moment, it leaves the possession of the proposed sender, or after, or at the moment, it comes into possession of the intended receiver."[10] In other words, implicit in the concept of "intercept" is that it must occur in the course of transmission.

4.18 We hold the view that the focus should be on interception in the course of transmission, rather than extending the offence to cover unauthorised access before or after transmission. We believe that it is necessary to delineate clearly the types of interception which merit additional controls on the basis of the gravity of their intrusiveness. In our view, interception in the course of transmission, and the immediacy of intrusion in these circumstances, falls into this category. Whilst the sender or receiver can take such steps as are necessary to safeguard a message against unauthorised interference before it is sent out or after it is received, they may not have the means to secure the message while it is being transmitted by a third party outside their control.

4.19 The United Kingdom, New Zealand and Australian legislation adopt the same approach.[11] Section 6(1) of the Australian Telecommunications (Interception) Act 1979 provides:

> *"For the purposes of this Act ... interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication."* [our underlining]

4.20 The New Zealand Crimes Act 1961 prohibits the use of listening devices to intercept a private communication "while it is taking place". Similarly, the United Kingdom Act restricts the offence to "intentionally intercept[ing] a communication *in the course of its transmission*."[12]

4.21 Even if it is accepted that the focus should be on interception in the course of transmission, drawing the line is not always easy. The scope of "interception" is clear enough with ordinary mail, and would cover reading, taking a copy, or delaying transmission. If A sends B a sealed letter and prior to delivery it is opened and read by C, this would clearly constitute an interception because the communication was still in the course of its transmission in a form which did not envisage its being read by others. However, it is arguable that the opening by an occupier of a letter addressed to another person at that address would constitute interception, notwithstanding the fact that the formal delivery had been completed. Much

---

10 *Black's Law Dictionary* (Minn: West Publishing Co, 6th ed, 1990), at 811.

11 The Canadian Criminal Code is not so restricted. Section 184(1) simply provides that every one who, by means of any specified device, wilfully intercepts a private communication is guilty of an offence. However, *Martin's Criminal Code* comments that the term "intercept" "must be interpreted in context and in accordance with its primary dictionary meaning as an interference between the place of origination and the place of destination of the communication." See *Martin's Criminal Code 1995*, at CC/263.

12 Interception of Communications Act 1985, section 1.

depends on whether the postbox to which the letter is delivered is used by the addressee or shared by a number of people. Whereas delivery is complete if the letter is delivered to a postbox used solely by the addressee, the letter would still be in the course of transmission if the postbox is shared by a number of people of which the addressee is one. On the other hand reading a postcard during the course of its transmission through the post would probably not constitute an "interception" because no efforts have been made by the sender to exclude this eventuality. An analogous situation would be where someone browses over faxes that have piled up in the addressee's absence.

"Interference"

4.22 We note that "interference" rather than "interception" of correspondence is protected under article 17 of the ICCPR. Nowak explains that:

> *"Every withholding, censorship, inspection of (or listening to) or publication of private correspondence represents 'interference' within the meaning of Art. 17 [of the ICCPR]."*[13]

4.23 One of the meanings of "interference" offered by the New Shorter Oxford English Dictionary is:[14]

> *"Disturbance of the transmission or reception of radio waves by extraneous signals or phenomena; signals etc. causing such disturbance; unwanted effects arising from such disturbance."*

4.24 In some respects, "interference" has a wider ambit than the definitions of "interception":

- Unlike "interception", "interference" may occur once the course of transmission has been completed. Whereas listening to a call or opening an undelivered letter would constitute "interception", reading a transcript of the completed call or the delivered letter may well constitute "interference."

- "Interference" would extend to the destruction, corruption or diversion of the communication, without necessarily becoming acquainted with its contents.

---

13 M Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), at 304.

14 The New Shorter Oxford English Dictionary defines "interfere" as follows: *"Of a person or persons: enter into something without right or invitation, or intending to hinder or obstruct ... Intervene so as to affect an action. ... Of light or other waves: mutually act upon each other and produce interference ... Broadcasting. Transmit a signal which is received simultaneously with the signal sought by the receiver".* In a United States decision "interfere" was defined as meaning: *"to check, hamper, hinder, infringe, encroach, trespass, disturb, intervene, intermeddle, interpose. To enter into, or to take part in, the concerns of others."* See *People ex re. Benefit Ass'n of Railway Employees v. Miner* 387 Ill. 393, 56 N E 2d 353, 356.

4.25 Whilst we wish to restrict the focus to protection during the course of transmission, we are concerned to regulate the destruction, corruption or diversion of the communication occurring during its transmission. As the terms "intercept" and "interfere" taken singly may not suffice, the law should prohibit both interference and interception of communications and the term "interference" should be defined as including destruction, corruption or diversion of communications.

4.26 We conclude that communications should be safeguarded from interception or interference (including destruction, corruption or diversion) in the course of their transmission.

"Communication"

4.27 Similarly vague is the ambit of "communication". Under the United Kingdom Act "communication" is not defined but was envisaged by the White Paper as encompassing "all forms of communications, whatever their nature, passing through these systems, such as letters, telephone calls, telex messages and telegrams, and other forms of electronic transmission like computer data or facsimile."[15] New telecommunications technologies enable users to send complex information objects, not just simple messages. Such objects may contain voice, video, fixed image and text information in a structure known only to the users.

4.28 At some stage a "communication" may lose that quality and become a record (a delivered letter could be an example), or the "communication" may become a record simultaneously with its being (separately) transmitted. Modern technology has negated the conceptual distinction between the transmission of data and its storage. For example, the telephone company will record a fax message in its computer while they attempt (perhaps repeatedly) to transmit the message to the recipient. If a telephone company official reads the recorded version the question arises whether this would constitute interception of "the communication". It may be necessary in this situation to distinguish the communication from its recorded back-up.

4.29 These examples also indicate that communications by mail and by telecommunications may raise different issues. One reason is that mail is a tangible object and accordingly misappropriation of a letter both during and following delivery would constitute theft. We note that the Post Office Ordinance contains a number of offences protecting mail, whether or not it is in the course of transmission. The Ordinance is not limited to public mail systems and we agree that both public and private courier systems should be protected, notwithstanding that contractual protections would apply in any event.

---

[15] *The Interception of Communications in the United Kingdom,* (Cmnd 9438, 1985), paragraph 12(a).

What types of communication ought to be protected?

4.30 Article 17 of the ICCPR provides protection for "correspondence" rather than communication. However, as we have already noted "correspondence" can include types of communication other than the written word. Nowak observes that:

> *"Although 'correspondence' [in article 17] primarily means written letters, this term today covers all forms of communication over distance, i.e. by telephone, telegram, telex, telefax, as well as by other mechanical or electronic means of communication."*[16]

4.31 In examining what types of communication ought to be protected, we have been influenced by the principles we have already set out in paragraph 55:

> *"Insofar as the individual has a reasonable expectation of privacy in the use of certain communications, he is entitled to have, in accordance with the ICCPR, an expectation that the privacy of such communications will be governed by the rule of law and that the law will protect such communications from any arbitrary or unlawful interference."*

4.32 Additionally, we are influenced by the practicality of regulating particular means of communication under consideration.

4.33 The application of these principles leads to clear - even obvious - results when applied to certain means of communication. It would be absurd to seek to regulate the interception of face-to-face speech in public, or shouting from hillside to hillside. Similar considerations apply to messages communicated by flag, smoke, drum or flashing light. Not only do the users of such means have no reasonable expectation of privacy but banning interception of, or interference with, them is not practical.

4.34 By the same principles, those who use any form of telecommunications or sealed letters do reasonably expect that their messages will be private and free from interception or interference in the course of transmission. The difference in the application is well illustrated by applying the principles to a postcard on the one hand, and a sealed letter on the other. The postcard fails the tests, even if the writer would prefer it not to be read in the course of transmission. The sealed letter satisfies them.

4.35 Their application to radio communication does not lead to such clear-cut results. The following are two extremes:

---

16 *Op cit*, at 304.

(a) a broadcast, where the intention is that the message contained in the communication can be received by as many people as possible;

(b) a communication from point A to point B, where the sender intends the message to be received only by the intended recipient but not others.

4.36 In applying the principles above, we are able to make the following observations:

(a) There is no reasonable expectation that a radio communication transmitted on an *unlicensed* frequency will be protected either from interference or interception.

(b) Whether a person transmitting a radio communication on a *licensed* frequency has a reasonable expectation that its transmission will not be the subject of interference or interception depends on the type of the licence.

(c) If the licence is for transmission on a broadcast frequency, then there can be no expectation that a communication using that frequency will not be received by anyone who is able to tune to that station.

(d) If the licence is for transmission on a restricted frequency in the sense that the licensed frequency is intended for use by certain individuals or organisations to communicate from point A to point B, there is a reasonable expectation that the radio communication will not be received by persons other than those who are licensed to use that frequency.

4.37 Thus, if a person uses a domestic cordless telephone or intercom equipment which has a very low radiated power, he can have no expectation that his communications transmitted on such public frequencies would not be intercepted by others. Similarly, communications on police frequencies should not be intercepted even though they are not encrypted because such communications are intended to be received only by the police. It was suggested to us that the police seem to be happy with the widespread practice adopted by the media in Hong Kong of intercepting police frequencies which are not encrypted, and that an exception should therefore be made. We are not sure that this is true, but if it is then presumably the media can obtain the necessary consent from the police without the enactment of a specific exception.

4.38 We conclude that when the use of a particular means of communication has a reasonable expectation of privacy and when it is practicable to regulate interception of or interference with that means of communication in the course of transmission, any such interception or interference ought to be controlled by law.

4.39 In practice, as in other common law jurisdictions, as a minimum there should be offences covering interception or interference with :

(a) telecommunications;
(b) sealed correspondence; and
(c) transmissions by radio on frequencies which are not licensed for broadcast.

"Telecommunications" include by their nature facsimile transmissions, data transmissions and communications over the Internet. As far as radio communication is concerned, the controls may be effected by specifying in the legislation the frequency bands which are considered as broadcast or restricted frequencies.

Controls in other jurisdictions

4.40 Other common law jurisdictions focus on the interception of mail and/or "telecommunications systems". For instance, section 7(1) of the Australian Telecommunications (Interception) Act 1979 provides that a person shall not intercept a communication *passing over a telecommunications system*.[17] Similarly, section 1 of the United Kingdom Interception of Communications Act 1985 creates a criminal offence where a person "intentionally intercepts a communication in the course of its transmission by post or by means of a *public telecommunication system*".

4.41 Although the United Kingdom Act is broader than the Australian Act because it encompasses both postal and telecommunications systems, it is also true that the former is narrower than the latter because the United Kingdom provisions do not prohibit interceptions of telecommunications which are not transmitted by a "*public* telecommunication system".

4.42 The ambit of the phrase "public telecommunication system" in the United Kingdom Act was considered in *R v Effik.*[18] In that case the appellants were indicted on counts of conspiracy to supply drugs. Part of the evidence against them consisted of recordings of telephone conversations. It was conceded that no warrant had been issued authorising the interceptions and that, if the interception was subject to the Act, the evidence obtained thereby would be inadmissible.

4.43 The intercepted call occurred with a cordless telephone which comprised a handset (consisting of a mobile battery operated transmitter/receiver) and a base unit. The handset can be used as a mobile within a limited range of the base unit. The base unit was in turn connected

---

17 "Telecommunications system" is defined as meaning:*"(a) a telecommunications network that is within Australia; or (b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia; and includes equipment, a line or other facility that is connected to such a network and is within Australia"*: section 5(1).

18 [1994] 3 WLR 583.

(through a telephone socket) to the British Telecom ("BT") system. The Court accepted that the BT system was "a public telecommunication system", having been designated as such by a statutory order. However, the signals were not intercepted within the BT system, but when transmitted between the base unit and the handset. The interception of these signals was effected by a radio broadcast receiver connected to a radio cassette recorder in adjoining premises. The Court accepted that the cordless telephone was approved for connection to the BT system, but held that it was not part of the BT network, which terminated at the junction box in the customer's premises. The telephone did not comprise part of a "public telecommunication system", as it was part of a privately run system. Furthermore, section 10(2) envisaged "that a communication by means of more than one telecommunication system is statutorily, if perhaps somewhat artificially, treated as temporally split in transmission between the various systems through which it may be transmitted." So, in the case in question, the interception was of signals being transmitted outside a public telecommunication system.

4.44 The more difficult issue was whether the interception nonetheless fell within section 1 as being "in the course of its transmission ... *by means of* a public telecommunication system." The Court was not assisted by a literal analysis and had to look at the presumed intention of the legislation. It concluded that the interception did not fall within section 1 because the policy of the Act was:

> "*to protect the integrity of that system of communication which is under public, and not under individual, control by creating a specific offence of interception of communications through the public system ... It was not an Act designed nor does it purport to confer any general protection against eavesdropping or intrusion on the privacy of individuals or to provide for any general authorisation for telephone tapping on private premises.*"[19]

4.45 In the result, the court held that the Act did not prohibit the interception and the interception was therefore legal. Even before *Effik* it was clear that the Act did not apply to eavesdropping which did not involve the interception of telephone calls. When moving the second reading of the Bill, the Secretary for State said that "bugging and other forms of surveillance were not covered by the legislation." In *R v Khan*[20] the House of Lords affirmed that the legislation was not applicable when considering the admissibility of evidence obtained by bugging private premises. Lustgarten and Leigh describe the Act's inapplicability to "a whole gamut of possible techniques involving variants on bugging" as "the biggest single loophole." By way of contrast, while the Australian Act focuses on telecommunications systems, it is supplemented at the state level by legislation regulating the use of listening devices.[21]

---

19 [1994] 3 WLR 583, at 592.

20 [1996] 3 WLR 162 at 171D-H.

21 E.g. Listening Devices Act 1972 (South Australia).

4.46 One of the reasons given in *Effik* for its narrow approach was that:

> *"The individual who connects his own private apparatus to the public system has means at his disposal to protect that apparatus from interference. What he cannot protect himself from is interference with the public system without which his private apparatus is useless. Hence the necessity for statutory protection of that system."*[22]

4.47 It should be noted that "public system" in this context does *not* mean one available to the public, but something much more specific, namely a system *designated* as a public system by statutory order. The Act's distinction between "public" and "private" systems hinges on whether or not the system is licensed. This distinction is not relevant in a privacy context.

4.48 The United States does not restrict the scope of its legislative control to public telecommunications systems. The interception of a cordless conversation, even the radio portion between the handset and the base unit, also requires a warrant.[23]

4.49 Similarly, the current controls in Hong Kong do not focus on public telecommunications systems. In fact, neither section 27 nor section 33 of the Telecommunication Ordinance makes any reference to telecommunications *systems* as such. We note that the European Court in the *Malone* case made no distinction between public and private telephone systems. An ordinary person using a communications system has no way to protect his communication from interference, irrespective of whether the system is public or not.

4.50 We therefore conclude that communications should be safeguarded from interception or interference, whether or not the communications system is public.

4.51 In our view, the protection of the integrity of the *systems* themselves raise public interest issues which are distinct from those involved in the protection of specific communications transmitted by such systems. These are well stated by the President of the United States Telephone Association, who comments that if the public becomes nervous about using the public network for fear of being tapped, that fear will translate into reduced use of the system, reducing revenues and denying participation in the information age.

---

22 [1994] 3 WLR 583, at 592.

23 *Privacy Journal,* October 1994.

Focus on communications systems inadequate

4.52 Having concluded that communications transmitted by a communications system should be protected from interference or interception, we have considered whether such a provision is sufficient.

4.53 We consider Hong Kong should not follow the United Kingdom in restricting the focus on the integrity of communications systems. Such an approach is too narrow as it denies protection to communications intended to be private which fall outside such systems. Communications transmitting from a speaker phone to the intended recipient, for example, should be protected even though they are not transmitted by any communications system. For the same reasons, consideration should also be given to protecting face to face communications.

4.54 Our view is that the reasonable expectation test should also apply to communications which are not transmitted by a communications system and whether they are communicated within or without private premises. We accordingly recommended in the consultation paper that the interception of communications by means of a technical device should be prohibited provided that the interception could not have been effected without the use of a technical device.[24] As the use of a technical device to intercept communications raises issues similar to those relating to intrusion into private premises, we have decided that our deliberations on the interception of communications not transmitted by a communications system be deferred to the report on surveillance.

4.55 We pointed out earlier that it is essential to adopt an integrated approach in dealing with the interception of communications and intrusion into private premises.[25] These two topics are not separate and distinct; they overlap with each other in situations where communications within premises are intercepted by means of a surveillance device. Our deliberations on the protection of communication privacy are therefore incomplete until we have examined in our report on surveillance how the use of a technical device to intercept communications should be regulated.

Proposed offence

4.56 Bearing in mind paragraph 4.39 above, **we recommend that it should be an offence intentionally to intercept or interfere with -**

(a) a telecommunication;
(b) a sealed postal packet; or
(c) a transmission by radio on frequencies which are not licensed for broadcast,

---

[24] Paragraph 5.45 of the consultation paper.

[25] See paragraphs 40 to 44 in the Introduction on the importance of adopting an integrated approach.

while the telecommunication, postal packet or radio transmission is in the course of transmission.

4.57 **We recommend that "interference" for the purposes of the proposed offence should include destruction, corruption or diversion.**

4.58 As far as other types of communication, such as postcards or transmissions on broadcast frequencies, are concerned, although it is not reasonably expected that the contents of such communications would not be intercepted, they should nevertheless be protected against interference by third parties. We note that existing legislation provides some protection against interference with communications which affect the integrity of the communications system. For example, a person who wilfully secretes or detains a postcard would be guilty of an offence under section 28 of the Post Office Ordinance (Cap. 98). It is also an offence under section 27 of the Telecommunication Ordinance (Cap. 106) for a person to interfere with a telecommunication installation with intent to prevent or obstruct the transmission of a message. Our proposed offence would supplement these provisions and offer better protection to communications utilising a communications system.

4.59 **We recommend that anyone who contravenes the proposed offence should be liable to a fine or a term of imprisonment not exceeding 5 years, or both.**

4.60 We note that intercepting the contents of a message stored by a telecommunications service provider while it is in the course of transmission would be governed by the provisions of the Personal Data (Privacy) Ordinance as well as by the law prohibiting the interception of communications recommended above.[26] We do not think there is a problem with such an overlap. The data protection law provides that personal data should be collected by means which are lawful and fair.[27] However, it does not impose any criminal sanctions on the person who has collected personal data by an interception of communications. As interception of communications without authority is an unfair means of collecting information, creating an interception offence is consistent with the principles underlying the data protection law. The offence would supplement the existing law on the protection of personal data by providing that interception of communications is not only unfair but also unlawful. The Personal Data (Privacy) Ordinance and the proposed legislation on interception are therefore complementary to each other. Whereas the former puts the emphasis on the use and storage of personal data, the latter focuses on the collection of data (whether personal or not) transmitted by a communications system. They both belong to a regime which safeguards the privacy of the individual.

---

[26] Cf paragraph 4.28 above.

[27] Cap. 486, schedule 1, data protection principle 1.

Interceptions by the private sector

4.61 The Hong Kong Journalists Association, whose principal concern appears to be surveillance, objected to the proposals of the Privacy sub-committee insofar as they affected interceptions by the private sector. The Association believed that the law relating to private sector tapping should remain unchanged. The following are their grounds of objection:

(a) there is no demonstrated need for criminal sanctions.
(b) compared with other common law jurisdictions, the definition of the proposed offence is too wide.
(c) there is no public interest defence.

4.62 In our opinion, interception of communications is an invasion of privacy whether it is initiated by the Government or by the private sector. The fact that Government interceptions may lead to prosecution does not make interceptions effected by the private sector less intrusive.

4.63 Article 17 of the ICCPR confers a right to be free from arbitrary or unlawful interference, whether such interference comes from the public authorities or the private sector. The United Nations Human Rights Committee comments that:

> *"States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal person."*[28]

4.64 The Government is therefore under an obligation to provide an appropriate regime which regulates violations by individuals and private organisations. We note that the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) apply to personal data collected or used by the private sector.[29] Indeed, the Basic Law expressly provides that "[no] department *or individual* may, on any grounds, infringe upon the freedom and privacy of communication of residents".[30]

4.65 We do not believe that the points raised by the Hong Kong Journalists Association are valid. We argued at the beginning of this chapter that there is a strong case for imposing criminal sanctions. The offence proposed in this report is also broadly in line with those in other jurisdictions. As regards the need for a public interest defence, this will be addressed in chapter 6 below.

4.66 We conclude that interceptions by individuals or private organisations should be prohibited and should not be exempted from the proposed offence.

---

28 General Comment 16/32 of 23 March 1988, CCPR/C/21/Rev 1(1989), paragraph 9.

29 Cf General Comment 16/32 of 23 March 1988, CCPR/C/21/Rev 1(1989), paragraph 10.

30 Article 30. The exceptions provided for in the Basic Law only apply to the "relevant authorities".

Interception with the consent of one party

4.67 Interception with consent mainly occurs in one of the following situations:

(a) a party to a private communication using a device to record it without the consent of the other party;

(b) a party to a private communication using a device to transmit the communication to someone who is not a party.

Other jurisdictions

4.68 Legislation elsewhere usually provides that it is a defence that *one* of the communicants consented to the interception. Hence, section 1(2)(b) of the United Kingdom Interception of Communications Act 1985 makes it a defence if the interceptor has reasonable grounds for believing that one of the communicants has consented.

4.69 In the United States, it is not unlawful for "a person acting under color of law" to intercept a communication, where such person is a party to the communication or one of the parties has given prior consent.[31]

4.70 The situation in Canada is more complicated. A person is not guilty of wilful interception by means of a surveillance device if one of the parties has consented.[32] But even if he has obtained the required consent, the interception would constitute an unreasonable search or seizure and would therefore be inadmissible in court under the Canadian Charter of Rights and Freedoms unless he has also obtained an authorization from a judge.[33] The effect of these provisions on the police is that they are required to obtain prior judicial authorisation even though one of the parties consents to the interception.

Australian Law Reform Commission

4.71 In a report on Privacy, the Australian Law Reform Commission examined the arguments for and against the regulation of participant monitoring involving the use of a listening device.[34]

---

31 Wiretap Act, section 2511(2)(c). Cf *United States v White*, 401 US 745, 28 L Ed 2d 453 and *Commonwealth v Schaeffer* 536 A. 2d 354, 365 (1987), Superior Court of Pennsylvania.

32 Criminal Code, section 184(2)(a).

33 Criminal Code, section 184.2(1).

34 Law Reform Commission of Australia, *Privacy* (Report No 22, 1983), paragraphs 1127-1135.

(a) Arguments for regulating participant monitoring

(i) The Commission observed that "unless [participant monitoring] is regulated, it could lead to honesty and frankness in discussion being compromised, and discussion itself becoming cautious and bland, losing its intimate, personal and informal character."[35]

(ii) The party who surreptitiously makes a recording can present matters in a way that is entirely favourable to himself because he is able to manipulate the conversation to his advantage.[36]

(b) Arguments against regulating participant monitoring

(i) Participant monitoring is used by many people to protect their private interests, particularly in commercial and business contexts. A prohibition on the use of devices for participant monitoring would fail to reflect contemporary practices and standards.

(ii) Tape recording of family events is a common practice in domestic and friendly circumstances. This conduct should not be subject to criminal sanctions.

(iii) A person speaking to another must take the risk that that other will make public what he has heard. Just as a party is free to make notes during or after the conversation, so he should not be prevented from recording the conversation as accurately as technology will allow.

(iv) There was no evidence of the harmful social effects that critics of participant monitoring suggested. Lack of regulation had not produced the chilling effects that some fear.

4.72 The Australian Law Reform Commission concluded that:

> *"to prohibit or otherwise regulate participant monitoring would be unnecessary and undesirable. To prohibit participant monitoring would lead to the result that a participant could take accurate and complete shorthand notes of a conversation and reproduce those notes with impunity, but would not be able to use a pocket recorder to perform exactly the same function."*[37]

---

35 *Ibid*, paragraph 1128.

36 As explained by the Canadian Law Reform Commission, "the knowing party can direct the conversation not only to draw out the suspect and make him incriminate himself, but at the same time may shield his own involvement and produce self-serving evidence : Law Reform Commission of Canada, *Electronic Surveillance* (Working Paper 47, 1986), at 27.

37 *Op cit,* paragraph 1133.

4.73 The Canadian Law Reform Commission agreed with the Australian Commission.[38]

Conclusions on interceptions with the consent of one party

4.74 One respondent to the sub-committee's consultation paper submitted that if a surveillance officer or undercover officer enters private premises lawfully without a warrant, he should be free to use a recording device carried on his person to obtain information therein without prior authorisation. This raises the question whether consensual interceptions should be regulated by law.

4.75 We consider that the law should focus on situations where none of the parties to the communication consents to the interception. It is only when no party consents that the interception amounts to an interference with the right to privacy. There is no question of interception as long as one of the communicants consents.[39]

4.76 It has been argued that it is beyond the expectation of the non-consenting party that his communications would be used as evidence. The non-consenting party, who is often in a weaker position, should be protected by a warrant system so as to minimise any possibility of abuse.

4.77 Those who are in favour of regulating consensual interceptions argued that widespread participant monitoring effectively bypasses any judicial scrutiny of the procedures prescribed in a regulatory framework. Dispensing with a warrant requirement if the interception is carried out with the consent of one of the parties would effectively allow the police to do indirectly what the law would prohibit them from doing directly. They claimed that, faced with the choice of having to apply for a warrant and persuading one of the parties to consent, it is likely that the police will, circumstances permitting, elect to proceed without a warrant. Moreover, if the public come to believe that participant monitoring is widespread, they may fall silent on occasions when they would have felt free to speak.

4.78 We acknowledge that there is a case for regulating consensual interceptions. However, the question as we see it is largely a matter of trust between the parties. If A engages in a conversation with B, he implicitly trusts B not to repeat the contents of the conversation to a third person. If A does not trust B, he should not have confided in B.

4.79 There is in principle no difference between making a written or oral report to a third party after the conversation, and making a permanent

---

[38] The Canadian Commission believed that "any attempt to regulate consent interceptions would be introducing an unnecessary complexity without any real gains in terms of accuracy of fact-finding or protection of legitimate privacy interests." Although the nature of the conversation may be distorted in favour of the knowing participant, expert evidence can be called at the trial to diminish the weight which the court should attach to a conversation. *Op cit,* at 28.

[39] However, if the information obtained relates to personal data, the use and storage of the data would be subject to the provisions of the Personal Data (Privacy) Ordinance.

electronic record during the conversation and then passing it on to a third party later. Insofar as a person may pass the written record on to a third party, he should also be allowed to transmit the conversation to a third party by using a hidden device.

4.80 Consensual interception is lawful in Hong Kong. It has always been lawful for a person to use a speaker-phone, thereby allowing a third party to listen to the whole conversation without the knowledge of the second party. The third party may subsequently give evidence as to the statements he heard. There is no real difference between a third party listening in to the conversation in such circumstances and surreptitious monitoring carried out with the consent of one of the parties.

4.81 In fact the use of the speaker-phone has reduced the expectation of privacy which a person may have when engaging in such telephone conversations. The device enables a third party to listen to the conversation without the knowledge of the second party. Whether the conversation is also recorded by the third party is not an issue. It is no longer a valid assumption that a telephone conversation will be heard only by the people who are allowed to listen to the conversation by one of the parties.

4.82 There is a difference in degree between surreptitious recording with the consent of one party and the making of notes during or after the conversation. Although the issues may be distorted if the consenting party has manipulated the conversation, that is a risk inherent in all conversations. Indeed, a person who makes a verbatim report of the contents of a communication may expand on what the participants had said. The use of a recording device by a communicant, albeit surreptitiously, would enable more reliable evidence to be obtained.

4.83 Material obtained by intercepting a communication with the consent of one party is a valuable source of evidence to the law enforcement agencies. Given that an undercover police officer can gain entry into private premises without a warrant simply by insinuating himself into the confidence of the suspect, there is no reason why he should not be allowed to record any communication to which he and the suspect are parties. We believe it would be impracticable to require either the consent of all parties or a warrant from the court before a recording may be made.

4.84 We endorse the following views expressed by the Canadian Court of Appeal in the case of *R v Duarte*:[40]

(a) The consent to the interception by the recipient may be looked upon as no more than an extension of the powers of recollection of the recipient of the communication.

---

[40] The decision of the Court of Appeal was overruled by the Canadian Supreme Court. The latter held that surreptitious interception of a private communication by agents of the state, though not unlawful under the Criminal Code, constitutes an unreasonable search or seizure under the Canadian Charter of Rights and Freedoms unless there is prior judicial authorisation or all parties have expressly consented to it: *R v Duarte* (1990) 53 CCC (3d) 1 at 21e.

(b) The person who divulges any confidence always runs the risk that his interlocutor will betray the confidence. The risk that an interlocutor will divulge one's words and the risk that he will make a permanent electronic record of them at the behest of the state are of the same order of magnitude.

(c) Consensual interception is inherently less offensive than third party monitoring because the agent of the state hears nothing that his interlocutor did not intend him to hear.

(d) The device is used merely to obtain the most reliable evidence possible of a conversation in which the agent of the state was a participant. It was carried in and out by an agent who was there with the suspect's consent, and it neither saw nor heard more than the agent himself.

(e) Just as the police are not subjected to any warrant requirement in their use of informers or in their efforts to insinuate themselves into the confidence of a suspect, the use of electronic surveillance, as an adjunct to that process, is of no constitutional significance.

4.85 On balance, we are not in favour of regulating consensual interceptions. We agree that consensual interception may be immoral and offensive in certain circumstances. However, such conduct should not be made criminal merely because it does not measure up to a high moral standard. The defence of consent should therefore be available to a person who is charged with the proposed offence. The consent must of course be real and not obtained by fraud. In formulating such a defence, we prefer the United Kingdom formulation, which provides that it is a defence if the interceptor has reasonable grounds for believing that a communicant has consented.

4.86 **We recommend that a person should not be guilty of the proposed offence if one of the parties to the communication has consented to the interception.**

Interception of communications by employers

4.87 Communications received by employees may be work-related or private. Whereas an employer may intercept a communication which is work-related, he would be liable for an offence under our proposals if it is a private communication. A letter addressed to an employee which is marked "private and personal" on the envelope is no different from ordinary mail sent to his home. As an employee retains the right to receive such letters without any unlawful or arbitrary interference, an employer who intercepts such letters should be liable unless he has the express or implied consent of the employee concerned. This accords with the reasonable expectation of the individual. It will be recalled that over 80% of the respondents to the survey

carried out in Hong Kong to which we referred earlier would be either very concerned or extremely worried if a letter sent to them marked "personal" were opened by their employers. We should add by way of clarification that we do not intend that the employer's right to intercept his employee's mail should extend to circumstances of domestic employment. It would clearly be quite wrong for an employer to intercept the mail of his domestic employee. In those circumstances, all mail addressed to the employee must be presumed to be personal and private.

4.88 Difficulties arise where the communication is transmitted by electronic mail. An employee who has an electronic mail account in his office may communicate with his friends for private purposes while in the office. Would the employee be considered as having consented to the employer intercepting his electronic mail so that the employer would not be liable for intercepting his communications? The fact that the computer through which private communications are received is provided by the employer cannot in our view form the basis for arguing that the employer is entitled to intercept the employee's electronic communications.

4.89 As an employee is generally expected to devote all his working hours to performing official duties and a letter addressed to a company is normally treated as official unless the envelope indicates otherwise, we are of the opinion that in general all employers are implicitly authorised to open and read all incoming communications (including electronic mail) unless it is clear in the circumstances that the communication is intended to be private. In other words, a communication addressed or directed to a company should be presumed work-related unless words like "private" or "personal" are marked on the cover (or shown in the subject heading where it is an electronic communication).

4.90 We consider that it is generally undesirable for an employer to have a system of opening and reading all incoming communications. Although private communications addressed to a place of employment would be protected by the law implementing our proposals, we are of the opinion that it is important that the right of an employer to intercept employee communications is made known to the employee before he takes up employment. Furthermore, an employer should not be liable for an offence unless the communication is clearly marked "private" or "personal". It is therefore important that the contract of employment should be sufficiently clear in its terms in clarifying what the employer can and cannot do so that both the employer and the employee know where they stand. It should state that all communications sent to the place of employment may be intercepted and read by the employer unless words like "private" or "personal" are marked on the cover (or shown in the subject heading where it is an electronic communication).

4.91 The employee who wants to safeguard the privacy of his communications should arrange for his private communications to be sent elsewhere. If he fails to do so, he would run the risk of his private

communications being intercepted and read by his supervisor or the company data base administrator if the sender omitted to indicate that it is private.

Interception of children's communications by parents

4.92 We have briefly considered whether interception of children's communications by parents should be exempted from regulation. A parent who cares for the upbringing of his or her child might wish to open and read the child's correspondence in order to ensure that he was not falling under undesirable influences. In the *Malone* case, the English court gave the example of "an anxious parent eavesdropping on a teenage child's conversation with an undesirable acquaintance by listening on an extension telephone". It could be assumed that interceptions by parents would normally be done with the best of intentions and with no criminal intent. It might therefore be thought somewhat heavy-handed if criminal sanctions were applied to such conduct.

4.93 Nevertheless, a child has as much right to privacy as an adult. The United Nations Convention on the Rights of the Child provides that no child below the age of 18 shall be subjected to arbitrary or unlawful interference with his or her privacy or correspondence, and that the child has the right to the protection of the law against such interference.[41] The ICCPR also provides that every child shall have "the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State".[42]

4.94 It is clear that interception or interference with a child's communications must not be arbitrary or unlawful and that a child is entitled to the protection of the law against undue interception or interference with his or her privacy or communications. We see no justification for derogating from the general right of protection we propose against interception of communications simply because one of the parties involved is a child. Equally, we think that reliance can safely be placed on the good sense and discretion of the prosecuting authorities to ensure that inappropriate prosecutions are not brought in such domestic circumstances. However, since what amounts to arbitrary or unlawful interference with children's communications raises social issues such as parental responsibility and the rights of the child, we suggest that the questions relating to the interception of children's communications be further examined by the Administration.

Interception to ensure compliance with licensing conditions

4.95 Telecommunication service providers are required to detect and eliminate radio interference and to ensure compliance with the licensing conditions. As these interceptions are necessary to ensure that the

---

41 Article 16. This Convention has been extended to Hong Kong.

42 Article 24(1).

telecommunication system is working properly, we agree that interceptions for these purposes should be exempted from regulation. We note that the Telecommunications Authority already has power to make tests and measurements of telecommunication apparatus to determine whether it complies with the requirements under the Telecommunication Regulations or the conditions of the licence under which it is held.[43]

4.96 **We recommend that a person should not be guilty of the proposed offence if the communication is intercepted for purposes connected with the prevention or detection of radio interference or for ensuring compliance with a licence issued under the Telecommunication Ordinance.**

Interception by telecommunication carriers for operational purposes

4.97 Hong Kong Telecommunications Limited want to be assured that the regulation of the interception or interference with communications would not hinder their operational ability to monitor their network.

4.98 Service operators have a duty to maintain the quality of service provided in the telecommunications network. They are also under an obligation to comply with the conditions of the licence granted under the Telecommunication Ordinance. For instance, they have to conduct interceptions in order to ensure that noise in the telecommunications network is maintained at an acceptable level. We therefore agree that service operators should be permitted to intercept telecommunications for the purpose of providing telecommunication service or carrying out mechanical or service quality control checks.

4.99 **We recommend that a person should not be guilty of the proposed offence if the communication is intercepted for purposes connected with the provision of telecommunication service or with the enforcement of any enactment relating to the use of that service.**

4.100 Although interceptions connected with the provision of telecommunication service should be exempted, there should be safeguards against any unauthorised interception carried out under the pretext that it is merely a technical interception done for operational purposes.

4.101 We hold the view that interception for operational needs is a matter to be controlled by the Telecommunications Authority through the licensing system. The Authority should specify in the licence the circumstances under which interceptions may be made for operational purposes. It should also lay down the extent to which such interceptions are required.

---

[43] Cap 106, sub leg A, regulation 12.

4.102 At present, licences granted under the Telecommunication Ordinance are not available to the public for inspection. There is no means by which the public can find out whether or not a particular interception made by the service operator is a technical interception covered by the licence. We think that all the terms of the licences governing the conduct of technical interceptions should be made public so that such interceptions would not be used as a backdoor means to unauthorised interceptions made without any legislative controls.[44] If it is specified in the licence that routine monitoring is scheduled to start at 4:00 p.m. every Friday, the operator will have no authority to carry out an interception at 9:00 a.m. on a Tuesday morning. By disclosing the relevant terms of the licence, the users of the telecommunication service would be able to find out how such interceptions would be made for the authorised purposes.

4.103 **We recommend that the Telecommunications Authority should specify in the licences granted under the Telecommunication Ordinance the circumstances under which and the extent to which interceptions for operational purposes may be carried out.**

4.104 **We recommend that the terms and conditions of licences which specify the circumstances under which and the extent to which interceptions for operational purposes may be carried out should be made available to the public for inspection.**

Use and disclosure of intercepted information

4.105 We have briefly considered whether criminal offences along the following lines should be created to supplement the proposed offence :

(i) unauthorised use or disclosure of information obtained as a result of intercepting a communication pursuant to a warrant; and

(ii) use or disclosure of information obtained as a result of intercepting a communication in contravention of the provisions prohibiting interception of communications.[45]

4.106 Where a person discovers that the intercepted material contains personal information relating to him and has been used or is being used for a purpose other than that for which a warrant was granted, he may lodge a complaint to the Privacy Commissioner appointed under the Personal Data (Privacy) Ordinance (Cap. 486) alleging that the use of the material contravenes data protection principle 3.[46] Provided that the data user:

---

[44] Schedule 3 to the Telecommunication Regulations contains the standard terms of the licences granted by the Authority: see regulation 2(7).

[45] The use or disclosure must be wilful and the accused must have knowledge that the material was intercepted in contravention of the provisions prohibiting interception of communications.

[46] Personal Data (Privacy) Ordinance, section 37(1). Data protection principle 3 provides that personal data shall not be used for any purpose other than the purpose for which the data

"(a) is contravening a requirement under [the Personal Data (Privacy) Ordinance]; or

(b) has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated",

the Commissioner may serve on the data user an enforcement notice directing him to take such steps as are specified in the notice to remedy the contravention.[47] However, no enforcement notice can be served if it is unlikely that the contravention will continue or be repeated.

4.107 The purpose of an enforcement notice is to remedy the contravention and not to penalise the person who has contravened the data protection principles. It is only when the data user fails to comply with the enforcement notice that he will commit an offence.[48] Where the user complies with the notice, for example, by ceasing to use or disclose the information for an unauthorised purpose, no criminal sanctions can be imposed on him in respect of the contravention.[49]

4.108 It should not be overlooked that personal data may be used in contravention of principle 3 if the use is exempted under Part VIII of the Ordinance. Thus, intercepted material may be used for the purposes of, *inter alia*, -

(a) the collection of tax or duty;
(b) the prevention of unlawful or seriously improper conduct;
(c) the prevention of significant financial loss arising from any imprudent business practices; and
(d) ascertaining whether the activities of the data subject are likely to have a significantly adverse impact on anything to which the discharge of statutory functions by the data user relates.

Disclosure of personal data to a person whose business consists of a news activity is also exempted if the discloser believes that the publishing of the data is in the public interest.

4.109 In the absence of any provisions prohibiting the use or disclosure of intercepted material, the material may be used or disclosed for any of the purposes permissible under Part VIII of the Ordinance provided

---

were to be used at the time of the collection of the data. The term "use", in relation to personal data, is defined as including disclosure or transfer of data.

47 Section 50. A contravention of a data protection principle is a contravention of a requirement under the Personal Data (Privacy) Ordinance: section 2(4).

48 Section 64(7).

49 The data subject may claim compensation if he suffers damage because of the contravention: section 66.

that it is not prohibited by the Telecommunication Ordinance[50] or the Official Secrets Act 1989 as extended to Hong Kong.[51]

4.110 Further, the provisions of the Personal Data (Privacy) Ordinance (including the data protection principles) have no application if the intercepted material does not contain any personal data (e.g. trade secrets).

4.111 The laws in Australia,[52] Canada,[53] New Zealand,[54] South Africa[55] and the United States[56] all contain provisions prohibiting unauthorised use or disclosure of intercepted material.

4.112 Although we are inclined to agree that such conduct should be subject to criminal sanctions, we have decided not to make any recommendation at this stage because any recommendation on the use and disclosure of intercepted material will inevitably impinge on our recommendations on surveillance. Whether a public interest defence should be available to the accused charged with unauthorised use or disclosure also requires to be examined.[57]

---

50 Section 24 of the Telecommunication Ordinance proscribes unauthorised disclosure of "message" by a telecommunication officer.

51 The Official Secrets Act 1989 applies to Hong Kong with adaptations and modifications. See the Official Secrets Act 1989 (Hong Kong) Order 1992, LN 207 of 1992. A person who is or has been a Crown servant or government contractor is subject to the provisions of the Act.

52 Telecommunications (Interception) Act 1979, section 63.

53 Criminal Code, section 193(1).

54 Crimes Act, section 312K.

55 Interception and Monitoring Prohibition Act 1992, section 7.

56 Wiretap Act, section 2511(1).

57 The question of whether a third party who intercepts a communication between two individuals is liable to either of them for breach of confidence will also be considered in our report on surveillance.

Chapter 5

Interception of communications authorised under existing legislation

---

Summary

5.1 This chapter considers the interception of communications under the following provisions :

- *Bankruptcy Ordinance (Cap. 6), section 28;*
- *Prison Rules (Cap. 234, sub. leg. A), Rules 47 and 48;*
- *Mental Health Regulations (Cap. 136, sub. leg. A);*
- *Import and Export Ordinance (Cap. 60), section 35(3); and*
- *Post Office Ordinance (Cap. 98), section 12.*

Recommendations

(A) Bankruptcy Ordinance (Cap. 6), section 28

5.2 Provisions should be made so that, wherever practicable, the debtor or his representative shall be given an opportunity to be present at the opening and examination of a postal packet re-directed, sent or delivered to the Official Receiver or trustee pursuant to an order made under section 28 of the Bankruptcy Ordinance.

5.3 In the event that the postal packet re-directed, sent or delivered to the Official Receiver or trustee pursuant to an order made under section 28 of the Bankruptcy Ordinance is found not to contain any information or material pertaining to the debtor's case, the Official Receiver or trustee shall either (a) forthwith return the packet to the debtor or his representative present before him, or (b) where the debtor has waived his right to attend, arrange for its delivery to the debtor without delay.

(B) Prison Rules (Cap. 234, sub. leg. A)

5.4 Subject to the Prison Rules and the Correctional Services Standing Orders being reviewed to take account of our views in paragraphs 5.20 and 5.21, the interception and monitoring of prisoners' communications under the Prison Rules should be exempted from the proposed regulatory framework.

(C) Mental Health Regulations (Cap. 136, sub. leg. A)

5.5 Subject to the Mental Health Regulations being reviewed to take account of our comments in paragraphs 5.57 to 5.59, the restrictions on communications to and from mental patients imposed under the Mental Health Regulations should be exempted from the proposed regulatory framework.

(D) Import and Export Ordinance (Cap. 60), section 35(3)

5.6 The power of the Postmaster General and the Commissioner of Customs and Excise to open and examine postal articles for the purpose of enforcing the provisions of the Import and Export Ordinance (Cap. 60) and the Dutiable Commodities Ordinance (Cap. 109) should be redefined along the following lines:

(a) The Post Office may detain a postal packet reasonably suspected to contain any dutiable goods or any goods which contravene any prohibition or restriction with respect to the import or export of goods.

(b) The postal article so detained shall be forwarded to the Commissioner of Customs and Excise.

(c) The Commissioner of Customs and Excise may open and examine the packet in the presence of the addressee. Where the addressee fails to attend after notice in writing requiring his attendance has been sent to him or if the address on the packet is outside Hong Kong, the packet may be opened and examined in his absence.

(d) If the Commissioner of Customs and Excise finds any goods as aforesaid, he may detain the packet for the purpose of taking proceedings with respect thereto.

(e) If the Commissioner finds no such goods, the packet shall be returned to the addressee.

5.7 Where it is not desirable for the packet to be opened or examined in the presence of the addressee, the Commissioner should apply for a warrant pursuant to the warrant system proposed below authorising him to open and examine it in the absence of the addressee.

(E) Post Office Ordinance (Cap. 98), section 12

5.8 The Postmaster General may open and delay a postal packet pursuant to section 12 of the Post Office Ordinance only if he has reason to believe that the postal packet has been posted or sent by post in contravention of the Post Office Ordinance.

(A) Redirection of debtors' correspondence under the Bankruptcy Ordinance

5.9 Section 28 of the Bankruptcy Ordinance (Cap. 6) gives the court a power to redirect a debtor's telegrams and postal packets to the Official Receiver or the trustee. It provides:

> *"Where a receiving order is made against a debtor the court, on the application of the Official Receiver or trustee, may from time to time order that for such time, not exceeding 3 months, as the court thinks fit telegrams and post letters and other postal packets, addressed to the debtor at any place or places mentioned in the order for re-direction, shall be re-directed, sent or delivered by the agent of the telegraph organization or the Post-master General, or the officers acting under them, to the Official Receiver or the trustee or otherwise as the court directs, and the same shall be done accordingly."*

One respondent commented that re-direction under these provisions should be exempted from regulation.

5.10 Section 28 of the Bankruptcy Ordinance was modelled on section 24 of the United Kingdom Bankruptcy Act 1914. An order under the section merely requires that the debtor's mail be re-directed, sent or delivered to the Official Receiver (or trustee). It does not expressly authorise the Official Receiver to open or read a letter or to censor its contents. Although Australia, Canada[1], New Zealand[2] and the United Kingdom[3] all have provisions similar to our section 28, there is a dearth of authorities in this area.

5.11 In a letter to the Privacy sub-committee, the Official Receiver advised that an application would be made if it is believed that a redirection of mail and telegram may be useful.[4] The application does not have to be supported by any documents. It appears that an order would be made solely on the basis that a receiving order has been made against the debtor. The re-directed mail would be opened, read and examined by the Insolvency Officer in charge of the case. After a letter has been read and, perhaps, censored, it will be returned to the debtor "as soon as possible". Applications for renewal are rarely made.

5.12 In commenting on the effectiveness of the making of an order, the Official Receiver advised that minor assets such as cheques are sometimes recovered. The existence of other creditors may also come to light. However, he accepted that such orders are not effective since debtors on the brink of bankruptcy usually have limited assets and far more effective means of communication are available than postal mail and telegram.

---

1 Bankruptcy Act (Chap B-3), section 17.

2 Insolvency Act 1967, section 67.

3 Insolvency Act 1986, section 371.

4 Between 1 May and 20 August 1996, 140 receiving orders were made but only 16 applications were made under section 28 of Cap 6.

5.13 There are basically two issues involved : (a) should the Official Receiver retain the power to apply for re-direction of debtors' mail; and (b), if so, should there be any safeguards against possible abuse of this power?

5.14 The monitoring of correspondence to a debtor against whom a receiving order has been made constitutes an interference with his right to privacy. However, we agree that the power under section 28 should be retained because it is necessary to protect the creditors against any action on the part of the debtor that could jeopardise recovery of the debts. Such measures may be justified on the ground that this is necessary to protect the interests of other persons.[5] The Official Receiver's Office will take appropriate action if the contents of a letter reveals that the debtor is hiding away assets which may be used to satisfy his debts.

5.15 An order under section 28 authorises the re-direction of *all* post letters and other postal packets addressed to the debtor. We agree that this is necessary because it is not possible to distinguish official correspondence from private correspondence unless and until a letter or packet is opened and read.

5.16 In order to safeguard the privacy interests of debtors, the debtor should be allowed to be present at the opening and examination of the postal packet if he so wishes. This would ensure that the debtor's packet would not be interfered with more than is necessary to determine whether it contains information or material pertaining to his case.

5.17 **We recommend that provisions should be made so that, wherever practicable, the debtor or his representative shall be given an opportunity to be present at the opening and examination of a postal packet re-directed, sent or delivered to the Official Receiver or trustee pursuant to an order made under section 28 of the Bankruptcy Ordinance.**

5.18 **We recommend that in the event that the postal packet re-directed, sent or delivered to the Official Receiver or trustee pursuant to an order made under section 28 of the Bankruptcy Ordinance is found not to contain any information or material pertaining to the debtor's case, the Official Receiver or trustee shall either (a) forthwith return the packet to the debtor or his representative present before him, or (b) where the debtor waived his right to attend, arrange for its delivery to the debtor without delay.**

(B) Communications of prisoners

5.19 One respondent to the sub-committee's consultation paper submitted that the interception of prisoners' correspondence and the monitoring

[5] *Santilli v Italy*, Application No 11634/85, 59 DR 81.

of prison visits by the Correctional Services Department under Rules 47 and 48 of the Prison Rules (Cap. 234, sub. leg. A) should be exempted.[6]

5.20 We agree that it would not be practicable for prisoners' communications to be subject to the regulatory framework proposed in the next chapter. However the Administration should review the Prison Rules and the Correctional Services Standing Orders in the spirit of our recommendations so as to give such latitude as is justified without undermining the need to maintain discipline and order in prison.

5.21 In conducting the review, regard should be had to -

(a) the human rights jurisprudence under article 17 of the ICCPR and article 8 of the European Convention as applied to prisoners' communications[7]; and

(b) the following international instruments:

(i) United Nations Standard Minimum Rules for the Treatment of Prisoners;[8]

(ii) United Nations Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment;[9] and

(iii) European Prison Rules.[10]

5.22 **We recommend that, subject to the Prison Rules and the Correctional Services Standing Orders being reviewed to take account of our views in paragraphs 5.20 and 5.21, the interception and monitoring of prisoners' communications under the Prison Rules should be exempted from the proposed regulatory framework.**

---

6 Rule 47 has recently been amended by the Prison (Amendment) Rules 1996, LN 300 of 1996.

7 E.g. *Golder v UK* (1975) 1 EHRR 524; *Silver v UK* (1983) 5 EHRR 347; *Campbell v UK* (1992) 15 EHRR 137. See also *R v Secretary of State for the Home Department, ex p Leech (No 2)* [1993] 3 WLR 1125; *Solosky v The Queen*, 105 DLR (3d) 745; *Procunier v Martinez*, 416 US 396; N Loucks, *Prison Rules : A Working Guide* (London: Prison Reform Trust, 1993).

8 UN Doc A/CONF/6/1, Annex I, A; adopted by the First United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 30 August 1955; approved by United Nations Economic and Social Council resolution 663 C(XXIV) of 31 July 1957; and amended by Economic and Social Council resolution 2076 (LXII) of 13 May 1977. The delegates in the General Assembly specifically stressed that the rules should be taken into account in interpreting and applying Article 10 of the ICCPR (on rights of persons deprived of their liberty).

9 United Nations General Assembly Resolution 43/173, Annex (1988).

10 Recommendation No R(87)3 of the Committee of Ministers of the Council of Europe adopted on 12 Feb 1987 at the 404th meeting of the Ministers' Deputies. The Rules are a revised European version of the UN Standard Minimum Rules for the Treatment of Prisoners. They serve as guidelines for the organs of the member states.

(C) Restrictions on patient communications under the Mental Health Ordinance

Introduction

5.23 A respondent to the sub-committee's consultation paper suggested that the power of medical superintendents to impose restrictions on mental patients under the Mental Health Regulations (Cap. 136, sub. leg. A) should be retained.

5.24 Our starting point is that every mental patient should have the right to exercise all civil and political rights as recognised in the ICCPR. In considering the provisions on patient communications in the Mental Health Regulations, we made reference to the rights of mental patients enshrined in the international instruments such as the *Declaration on the Rights of Disabled Persons*[11] and the *Principles for the Protection of Persons with Mental Illness and the Improvement of Mental Health Care*[12]. The latter provides that a mental patient has a right to freedom of communication which includes -

- freedom to communicate with other persons in the mental health facility;
- freedom to send and receive *uncensored* private communications;
- freedom to receive, *in private*, visits from a counsel or personal representative and, at all reasonable times, from other visitors; and
- freedom of access to postal and telephone services.

5.25 In coming to our recommendations, we have made reference to the laws in Australia,[13] Canada,[14] New Zealand,[15] the United Kingdom[16] and the United States.[17]

5.26 The provisions regulating communications of mental patients in Hong Kong can be found in the Mental Health Regulations as amended by the Mental Health (Amendment) Regulation 1996.[18] They cover three main areas: namely, written communications, visits and telephone calls.

---

11 Adopted at the 30th Session of the UN General Assembly on 9 December 1975.

12 Adopted by General Assembly resolution 46/119 of 17 December 1991.

13 E.g. Mental Health Act (Queensland) (No 2 of 1974), section 53; Mental Health Act (Tasmania) (No 63 of 1963), section 109; Mental Health Act (Victoria) (No 59 of 1986), sections 20 & 47.

14 See G B Robertson, *Mental Disability and the Law in Canada* (Carswell, 2nd ed, 1994), at 453-455.

15 Mental Health (Compulsory Assessment and Treatment) Act 1992, sections 73 & 74, 123-125.

16 Mental Health Act 1983, section 134. See L Gostin, *Mental Health Services - Law and Practice* (Shaw and Sons, 1986); R Jones, *Mental Health Act Manual* (Sweet and Maxwell, 4th ed, 1994).

17 See S J Brakel, J Parry & B A Weiner, *The Mentally Disabled and the Law* (American Bar Foundation, 1985), chapter 5.

18 LN 298 of 1996, gazetted on 5 July 1996.

Need for restrictions on written communications

5.27 There is evidence to show that freedom to communicate is conducive to early recovery of mental patients and that detention in mental hospital is harmful to the patient and unnecessary to public safety.[19] However some restrictions might be desirable to protect the innocent and to ensure that valuable family relations will not be harmed.[20] There is also a need to prevent the inflow of contraband into mental hospitals.[21]

Importance of visits and telephone communications to patients

5.28 Visits and telephone communications are essential means by which a patient receiving treatment at a mental hospital can maintain ties in the community outside the hospital. They enable mental patients to receive the much needed support from family, friends and other resources in the community.

5.29 Telephone communication is particularly important for a patient who is illiterate or cannot write because of his infirmity or disability. It is also important for those whose family and friends find visits difficult because of the location of the hospital, or impracticable due to the infirmity or disability of the visitor.

"Mental patients"

5.30 The regulations respecting patient communications apply to "any postal article or any other article or thing" addressed to or intended to be sent by a "patient". The meaning of "patient" in the Mental Health Ordinance (Cap. 136) is extremely wide. It means "a person suffering or appearing to be suffering from mental disorder".[22] In other words, the regulations apply to all patients in mental hospitals whether they are liable to be detained in the hospital or not.

5.31 Patients not detained in mental hospitals include: (i) patients admitted for the purpose of receiving treatment in a mental hospital but not liable to be detained therein, i.e. voluntary patients, and (ii) patients who are subject to guardianship.[23] Some countries make a distinction between patients who are liable to be detained in hospital and those who are not. The restrictions in the mental health legislation of New Zealand, for instance, apply only to persons who are required to undergo further assessment and

---

19 S F Adams, *The Committed Mentally Ill and Their Right to Communicate*, 7 WFLR (1971) 297.

20 Manitoba Law Reform Commission, *Report on Emergency Apprehension, Admissions and Rights of Patients under the Mental Health Act* (1979), at 47-51.

21 A contraband item may include items which the sender considers innocuous but may be dangerous to a patient who is admitted because of a possible suicide attempt.

22 Section 2.

23 Cap 136, sections 33 & 35.

treatment or who are subject to a compulsory treatment order.[24] In the United Kingdom, the restrictions mainly focus on correspondence with patients who are detained in "special hospitals" on account of their dangerous, violent or criminal propensities. A patient who is detained in a hospital not being a "special hospital" is not allowed to communicate in writing *only if* the addressee has requested that communications by him should be withheld. Patients who are not liable to be detained are not subject to any restrictions whatsoever. It is interesting to note that the statutes of a few states in Canada[25] go so far as to provide that a mental patient's mail must not be opened, examined or withheld. In the light of the experience overseas, we have reservations that patients not liable to be detained in hospital should be subject to the same set of restrictions as are applicable to those who are.

5.32 As regards patients detained in mental hospitals, they may be divided into 2 categories: those who have to receive treatment under conditions of special security on account of their dangerous, violent or criminal propensities and those who do not. Again we are not so sure that the latter category should be subject to the same set of restrictions as the former.

Outgoing articles

Power to open and examine articles

5.33 Under the Mental Health Regulations, any article sent by a patient may be opened and examined by a medical superintendent unless the article is addressed to a person or body specified in regulation 5(2), namely,

(a) the Governor;
(b) a public officer;
(c) a member of the Legislative Council;
(d) the Hospital Authority;
(e) the Mental Health Review Tribunal or its secretary; or
(f) a solicitor acting for the patient.[26]

5.34 We find it undesirable that a medical superintendent is *not* required to have any reasonable belief before he could open and examine an outgoing article.

5.35 The list of persons who are exempted from the restrictions is short compared with other jurisdictions. Two notable omissions are medical practitioners in private practice and the Commissioner for Administrative Complaints.

---

24 Mental Health (Compulsory Assessment and Treatment) Act 1992.
25 I.e. Alberta, Manitoba and the Yukon.
26 Regulation 5(1).

Power to withhold articles

5.36 A medical superintendent may withhold any article sent by a patient if-

(a) the addressee has given notice in writing to the medical superintendent requesting that such should not be sent; or

(b) the medical superintendent reasonably considers that such article is likely to

- cause danger to any person; or
- cause unnecessary distress to the addressee or to any other person, not being a person on the staff of the mental hospital.[27]

5.37 Articles addressed to persons specified in regulation 5(2) must not be withheld.[28]

5.38 Gostin comments that the "distress" criterion is vague, particularly as it applies to those who have not requested that the patient's post should be withheld.[29]

Power to delete any part of letter

5.39 Any part of a letter sent by a patient may be deleted if the medical superintendent reasonably considers that such part if not deleted would be likely to -

- cause unnecessary distress to the addressee or to any other person, not being a person on the staff of the mental hospital; or
- cause danger to any person.[30]

Duty to give notice and return articles to patient

5.40 Where an article sent by a patient is withheld or any part of a letter sent by him is deleted, the medical superintendent must within 7 days give notice of that fact to the patient and to the addressee.[31] The article must also be returned by the superintendent to the patient.[32] There is no requirement that the notice must give reasons for the withholding or deletion.

---

27 Regulation 5B(1).
28 Regulation 5B(2).
29 L Gostin, *Mental Health Services - Law and Practice* (1986, Shaw & Sons), para 24.31.2.
30 Regulation 5C(1)(b) & (c). Letters sent to persons specified in regulation 5(2) may not be deleted: regulation 5C(2)(a).
31 Regulation 5D(b).
32 Regulation 5E(b).

5.41 The medical superintendent is not under a duty to inform the patient and addressee if the article has been opened and/or examined but nothing is withheld or deleted.

Incoming articles

Power to open and examine articles

5.42 A medical superintendent may open and examine *any* article addressed to a patient which is sent to a mental hospital. As in the case of outgoing mail, he need not have any reasonable belief before exercising such power.

5.43 Articles sent by persons specified in regulation 5(2) are *not* exempted from this restriction and may be opened and examined as any other articles sent to the hospital.[33] This means that a letter from the patient's solicitor may be opened and examined as any other ordinary correspondence.

Communications with legal representatives

5.44 The United Nations *Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment* provides:[34]

> *"1. A detained or imprisoned person shall be entitled to communicate and consult with his legal counsel. ...*
>
> *3. The right of a detained or imprisoned person to be visited by and to consult and communicate, without delay or censorship and in full confidentiality, with his legal counsel may not be suspended or restricted save in exceptional circumstances, to be specified by law or lawful regulations, when it is considered indispensable by a judicial or other authority in order to maintain security and good order.*
>
> *4. Interviews between a detained or imprisoned person and his legal counsel may be within sight, but not within the hearing, of a law enforcement official. ..."*

5.45 Any patient who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. The objective of confidential communication with a lawyer cannot be achieved if a

---

33 Regulation 5.

34 UN General Assembly Resolution 43/173 (1988), Annex, principle 18. In *S v Switzerland,* 28 November 1991, E Ct H R, Series A, No 220, pp 15-16, the European Court of Human Rights stressed the importance of a prisoner's right to communicate with counsel out of earshot of the prison authorities.

medical superintendent has an unfettered discretion to open and examine a patient's legal correspondence without any cause.[35]

Power to withhold articles

5.46 A medical superintendent may withhold an article addressed to a patient if he reasonably considers that the article is likely to -

- cause unnecessary distress to the patient;
- adversely affect the treatment of the patient; or
- cause danger to any person.[36]

5.47 This provision allows the authority to withhold an incoming article under the "distress" criterion even though the article would not adversely affect the patient's treatment or cause danger to any person.

Power to delete any part of letter

5.48 Any part of a letter addressed to a patient may be deleted if the medical superintendent reasonably considers that such part if not deleted would be likely to -

- cause unnecessary distress to the patient;
- adversely affect the treatment of the patient; or
- cause danger to any person.[37]

Duty to give notice and return articles to sender

5.49 Where an incoming article is withheld or any part of an incoming letter is deleted, the medical superintendent must within 7 days give notice of the fact to the patient and to the sender.[38] The article must also be returned to the sender.[39] Where the sender is unknown, the superintendent only needs to notify the patient but not any other third party.

5.50 There is no requirement that the notice must give reasons for the withholding or deletion. The notice, as in the case of outgoing mail, is not required to be given in writing. The medical superintendent is not under a

---

35 *Campbell v UK* (1992) 15 EHRR 137, paragraph 50; *Solosky v The Queen*, 105 DLR (3d) 745 at 760, approved by the English Court of Appeal in *R v Secretary of State for the Home Department, Ex p Leech (No 2)* [1993] 3 WLR 1125 at 1140.

36 Regulation 5A(1). An article addressed by a person specified in regulation 5(2) must not be withheld except with the prior consent of that person: regulation 5A(2).

37 Regulation 5C(1)(a) & (c). Letters addressed to a patient by a person specified in regulation 5(2) must not be deleted unless the prior consent of that person is obtained: regulation 5C(2)(b).

38 Regulation 5D(a).

39 Regulation 5E(a).

duty to inform the patient and the sender if the article has been opened and/or examined but nothing is withheld or deleted.

5.51 The medical superintendent is not under a statutory duty to record the opening and inspection of post nor is he under a duty to record the grounds on which an article is withheld.[40]

Direction given by medical superintendent : regulation 9

5.52 A medical superintendent may direct that a patient is not to receive "any article or thing" if the medical superintendent reasonably considers that "the patient is of such unsound mind that he is incapable of looking after, handling or using the article or thing properly".[41] Any article or thing sent in contravention of such a direction may be confiscated by a medical superintendent.[42] We are concerned that this provision may be used by medical superintendents to get round the safeguards applicable to postal articles.

Visits

5.53 A medical superintendent may refuse to permit a person (other than a "mental hospital visitor" appointed under section 5 of the Mental Health Ordinance) to visit a patient if he reasonably considers that the visit is likely to-

- cause unnecessary distress to the patient; or
- adversely affect the treatment of the patient.[43]

5.54 A patient does not have a right to receive visits from his legal representative and a medical practitioner of his choice. There are also no provisions ensuring that interviews with mental hospital visitor,[44] legal representative and private medical practitioner[45] should be conducted in private.

---

40 Cf Mental Health Act 1983 (UK), section 134(5) and Mental Health (Hospital, Guardianship and Consent to Treatment) Regulations 1983 (UK), regulations 17 & 18.

41 Regulation 9(1).

42 Regulation 9(3).

43 Regulation 4(1).

44 The Governor may appoint mental health visitors for every mental hospital pursuant to section 5 of the Mental Health Ordinance. These visitors are under a duty to inspect the hospital and to "see and examine so far as circumstances permit", every patient therein.

45 See *Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment*, UN General Assembly Resolution 43/173 (1988), Annex, principles 18 and 29. The European Prison Rules, *op cit,* contain similar provisions.

Telephone calls

5.55 A medical superintendent may refuse to permit a patient to make or to receive a telephone call if -

(a) he reasonably considers that the telephone call is likely to -
- adversely affect the treatment of the patient; or
- cause unnecessary distress to (i) the patient, (ii) the person to whom the telephone call is made, or (iii) any other person, not being a person on the staff of the mental hospital; or

(b) the person to whom the telephone call is made has given notice in writing to the medical superintendent requesting that a telephone call made to him by the patient should be disallowed.[46]

Principles governing communications of mental patients

5.56 We agree that it is necessary for mental patients' freedom to communicate to be restricted in certain cases. However, there should be a system in operation which would ensure that their rights are protected.

5.57 Restrictions on communications should be imposed only if the medical superintendent reasonably believes that the communication is likely to be harmful to the patient or others. The medical superintendent should give his reasons for making an order restricting a patient's freedom to communicate. The order together with his reasons should be recorded in writing. It should be limited in time but the medical superintendent should have a right to renew or extend it if necessary. Whatever regulations that are put in force should conform with the international covenants.

5.58 The decision to restrict patient communication must be made by the medical superintendent after consultation with at least one medical practitioner. However, the following rights should not be limited or affected by his decision:

(a) the right to seek consultation with a medical practitioner of his own choice;

(b) the right to request a legal representative to advise him on his status and rights as a patient, or any matters on which persons customarily seek legal advice; and

(c) the right to communicate with any person to whom the patient has a statutory right of appeal.

---

[46] Regulation 4(2).

5.59 We are aware that access to a lawyer or a private medical practitioner is likely to be difficult for mental patients. It is therefore essential that any restriction should be subject to independent review by a person who does not belong to the establishment of the mental hospital. One possible option is to notify the mental hospital visitor or an independent psychiatric social worker every time a restriction is imposed. This would provide an opportunity for the visitor or social worker to scrutinise the restriction. Employing a tribunal to conduct the review is another option. However, a tribunal may not be an efficient way to handle such matters. The Administration may like to explore this matter further.

5.60 In view of what was said in the preceding three paragraphs, communications to and from mental patients should be exempted from the general regulatory framework but the Mental Health Regulations should be reviewed in the light of our comments made in this chapter.

5.61 **We recommend that, subject to the Mental Health Regulations being reviewed to take account of our comments in paragraphs 5.57 to 5.59, the restrictions on communications to and from mental patients imposed under the Mental Health Regulations should be exempted from the proposed regulatory framework.**

(D) Power to open and examine postal packets under the Import and Export Ordinance

5.62 We have examined whether the power to open and examine postal packets under section 35(3) of the Import and Export Ordinance (Cap. 60) should be retained. Section 35(3) provides:

> *"Any authorized officer or any member of the Customs and Excise Service may, in the presence of and under the directions of an officer of the Post Office, open and examine any postal packet held in the custody of the Post Office."*

5.63 Under the Post Office Ordinance (Cap. 98), the Postmaster General may open and delay anything the importation or circulation of which is forbidden in Hong Kong or in the country of destination,[47] or if the packet contains any dutiable article[48].

5.64 The power under section 35(3) is to open and examine "*any* postal packet held in the custody of the Post Office". "Postal packet" includes a letter because the term has the same meaning assigned to it under the Post Office Ordinance.

---

47 Provided that the country of destination is included in the Universal Postal Union: sections 12 and 32(g).

48 Section 12. "Dutiable goods" in the Dutiable Commodities Ordinance (Cap 109) means goods which are not exempt from duty and on which the full duty prescribed by law has not been paid.

5.65 The power to open and examine is vested in "any authorized officer or any member of the Customs and Excise Service". "Authorized officer" is broadly defined as "any person approved by the Secretary for Security, any public officer[49] and any police officer of the rank of Inspector or above" authorized by the Commissioner of Customs and Excise.[50] We consider that the persons authorized to open and examine packets should be more restricted.

5.66 It is important to draw a distinction between local mail and overseas mail and between letters and other postal packets. The treatment of local mail and overseas letters should be different from that of parcels and small packets addressed to a place outside Hong Kong because the former does not involve any customs issues. The main concern of customs officers is to check whether a postal packet addressed to a place outside Hong Kong contains any goods contrary to the import and export restrictions. The focus is on goods not letters. As there is no question of the officers reading the contents of a letter, the risk of privacy invasion is lower in such cases. This is especially so if the addressee were given an opportunity to be present at the opening and examination of the packet. Thus, whereas local mail should not be opened unless it is authorised by court, overseas mail may be opened by customs officers as a routine exercise to enforce customs laws against illegal activities.

5.67 Although it is not feasible to apply the warrant system to the regulation and control of the import and export of articles, we still have to examine if section 35(3) contains sufficient safeguards against arbitrary interference with privacy and correspondence.

5.68 We note that the baggage of any person arriving at or departing from the airport may be searched by customs officers without any ground of suspicion. The Dutiable Commodities Ordinance (Cap. 109) provides that any person entering or leaving Hong Kong must "on demand by any member of the Customs and Excise Service or police officer" permit his goods and baggage to be searched by such member or officer.[51] However, it further provides that the goods and baggage of a person who wishes to be present when they are searched must not be searched except in his presence. It appears that this practice is acceptable to the public.

5.69 In the United Kingdom, the Post Office may detain any postal packet suspected to contain any dutiable goods or any goods which contravenes any restriction on the import and export of articles. Section 17 of the Post Office Act 1953 provides:

> *"(1) ... , the Post Office may detain any postal packet suspected to contain any goods chargeable with any duty*

---

49 "Public officer" means "any person holding an office of emolument under the Crown in right of the Government of Hong Kong, whether such office be permanent or temporary": Interpretation and General Clauses Ordinance, section 3.

50 See Cap. 60, section 4.

51 Section 33(1).

charged on imported goods (whether a customs or an excise duty) which has not been paid or secured or any goods in the course of importation, exportation or removal into or out of the United Kingdom, contrary to any prohibition or restriction for the time being in force with respect thereto under or by virtue of any enactment and may forward the packet to the Commissioners of Customs and Excise.

(2) Where any postal packet has been forwarded to the said Commissioners under this section they may -

(a) in the presence of the person to whom the packet is addressed; or

(b) if, after notice in writing from them requiring his attendance left at or forwarded by post to the address on the packet, the addressee fails to attend, or if the address on the packet is outside the British postal area, then in his absence,

open and examine the packet.

(3) Where the said Commissioners open and examine a postal packet under this section, then -

(a) if they find any such goods as aforesaid they may detain the packet and its contents for the purpose of taking proceedings with respect thereto;

(b) if they find no such goods, they shall either deliver the packet to the addressee upon his paying any postage and other sums chargeable thereon or, if he is absent, forward the packet to him by post."

5.70 The Act does not require that the suspicion of the Post Office be reasonable. Although imposing a requirement of reasonable suspicion may render the task of postal officers more difficult to perform, we consider that a postal packet should not be opened unless a postal officer has reason to suspect that the packet contains any dutiable goods or any goods contrary to any import and export restrictions.[52] If there were no requirement of reasonable suspicion, the authorities would have carte blanche to open and examine any postal packet and an officer may target his operations against a particular person for his private purposes. Although a packet should be opened only if a postal officer has reasonable suspicion, the power to open and examine the packet should be vested in the customs officers because the subject matter with respect to the packet falls within the jurisdiction of the Customs and Excise Service.

---

[52] In fact, section 12 of the Post Office Ordinance provides that a postal packet may be opened only if the Postmaster General "has reason to believe" that it contains any dutiable article.

5.71 We also believe that the addressee should be given an opportunity to attend at the opening and examination of the packet. A notice in writing requiring his attendance should be given to him in advance. The packet may be opened and examined in his absence only if he fails to attend or the address on the packet is outside Hong Kong. Provided there is reasonable suspicion and the addressee is given an opportunity to attend, we have no objection to the customs officers opening and examining the packet without the authorisation of a warrant.

5.72 **We recommend that the power of the Postmaster General and the Commissioner of Customs and Excise to open and examine postal articles for the purpose of enforcing the provisions of the Import and Export Ordinance and the Dutiable Commodities Ordinance should be redefined along the following lines:**

(a) The Post Office may detain a postal packet reasonably suspected to contain any dutiable goods or any goods which contravene any prohibition or restriction with respect to the import or export of goods.

(b) The postal article so detained shall be forwarded to the Commissioner of Customs and Excise.

(c) The Commissioner of Customs and Excise may open and examine the packet in the presence of the addressee. Where the addressee fails to attend after notice in writing requiring his attendance has been sent to him or if the address on the packet is outside Hong Kong, the packet may be opened and examined in his absence.

(d) If the Commissioner of Customs and Excise finds any goods as aforesaid, he may detain the packet for the purpose of taking proceedings with respect thereto.

(e) If the Commissioner finds no such goods, the packet shall be returned to the addressee.

5.73 **We recommend that where it is not desirable for the packet to be opened or examined in the presence of the addressee, the Commissioner should apply for a warrant pursuant to the warrant system proposed below authorising him to open and examine it in the absence of the addressee.**

5.74 In circumstances where time is of the essence, the Commissioner may apply to the court for a warrant *ex post facto* under our proposals in chapter 6.

(E) Power of Postmaster General to open postal packets

5.75 Our discussion so far has not touched on the power of the Postmaster General to interfere with postal packets pursuant to the provisions of the Post Office Ordinance (Cap. 98). Although the warrant system set up under the United Kingdom Interception of Communications Act 1985 applies to communications transmitted by post, section 11(4) of the Act specifically provides that the provisions of the Act "[do] not affect any power conferred on the Post Office by or under any enactment to open, detain or delay any postal packet or to deliver any such packet to a person other than the person to whom it is addressed."[53] Our terms of reference oblige us to examine whether the provisions of the Post Office Ordinance provide sufficient safeguards against undue interference with individual privacy by the Postmaster General.[54]

5.76 Section 12 of the Post Office Ordinance provides that the Postmaster General may open and delay a postal packet if he has reason to believe that the packet-

(a) has been posted or sent by post in contravention of the Post Office Ordinance;
(b) contains anything which may not legally be sent by post;
(c) contains anything with respect to which or by means of which any offence whatsoever has been or is being committed or attempted; or
(d) contains any dutiable article.

5.77 In our view, the Postmaster General's power to open a postal packet if it contains "anything with respect to which or by means of which any offence whatsoever has been or is being committed or attempted" is too wide. We are of the opinion that its application should be restricted to offences under the Post Office Ordinance.

5.78 **We recommend that the Postmaster General may open and delay a postal packet pursuant to section 12 of the Post Office Ordinance only if he has reason to believe that the postal packet has been posted or sent by post in contravention of the Post Office Ordinance.**

5.79 It will be recalled that we recommended above that the power to open a postal packet suspected to contain a dutiable article should be transferred to the Customs and Excise Service.

---

[53] The 1985 Act contains only one consequential amendment to the Post Office Act 1953. Whereas formerly the Post Office may open a postal packet pursuant to "an express warrant in writing issued under the hand of a Secretary of State", section 58 now provides that the Post Office may open a postal packet "in obedience to a warrant issued by the Secretary of State under section 2 of the Interception of Communications Act 1985".

[54] The Hon James To commented that section 32 (offences relating to the sending of prohibited articles) should be amended so as to make it compatible with the Hong Kong Bill of Rights. We refrain from making any comments on the offences under section 32 because it is beyond the remit of the Law Reform Commission.

5.80 Where an offence other than one created under the Post Office Ordinance is involved, the Postmaster General should not be allowed to open the packet unless he has obtained a warrant issued by the court under our proposals. This would mean that the Postmaster General may open a postal packet under section 12 only if -

(a) the packet has been posted or sent by post in contravention of the Post Office Ordinance (no warrant is required in this case); or

(b) he obtains a warrant issued by the court authorising him to do so (in which case the sending of the packet would probably involve a serious crime).

Chapter 6

The regulatory framework

Summary

6.1 Having defined the offence regulating the interception of communications, we now consider the issues arising from a regulatory framework which consists of a warrant system.

Recommendations

(A) The warrant system

6.2 A warrant should be required to authorise all interceptions of communications falling within the scope of the proposed offence prohibiting these activities.

6.3 All applications for warrants for interception of communications should be made to a judge of the High Court.

6.4 The Postmaster General should have a power to delay a postal packet for such time as may reasonably be necessary for the purpose of obtaining a warrant authorising him to intercept postal packets.

(B) Grounds on which a warrant may be issued

6.5 A warrant may be issued if the interception is for the purpose of:

(a) preventing or detecting serious crime; "serious crime" should be defined by virtue of the maximum sentence applicable to the offence. The appropriate level of sentence should be determined by the Administration, but account should be taken of the need to provide a lower sentencing threshold for offences involving an element of bribery or corruption.

(b) safeguarding public security in respect of Hong Kong.

(C) No application by the private sector

6.6 Only the Administration and its law enforcement agencies may apply for a warrant authorising interception of communications. The

application should be made by a senior officer but it should be a matter for the Administration to decide which of its post-holders should be authorised to apply for a warrant.

(D) Form of application

6.7 An application for a warrant authorising interception of communications should be made in writing.

(E) Matters on which judge must be satisfied

6.8 A warrant authorising interception of communications should be issued only if the judge is satisfied that -

(a) there is reasonable suspicion that an individual is committing, has committed or is about to commit a serious crime, or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong; and

(b) there is reasonable belief that information relevant to the investigation will be obtained through the interception; and

(c) the information to be obtained cannot reasonably be obtained by less intrusive means.

6.9 In reaching a conclusion on the appropriateness of issuing a warrant, the judge should have regard to the following factors:

(a) the immediacy and gravity of the crime or the threat to public security in respect of Hong Kong, as the case may be;

(b) the likelihood of the crime or threat occurring; and

(c) the likelihood of obtaining the relevant information by the proposed interception.

(F) Information to be provided on application for a warrant

6.10 An application for a warrant authorising interception of communications should be accompanied by an affidavit. The information to be provided in the affidavit should include:

(a) the name, identity card number and rank or post of the person making the application;

(b) the facts relied upon to justify the belief that a warrant should be issued, including the particulars of the serious crime or the threat to public security in respect of Hong Kong;

(c) *the identity of the person, if known, whose communications are to be intercepted;*

(d) *a general description of the form of communications to be intercepted and the manner of interception proposed to be used;*

(e) *the nature and location of the facilities from which the communication is to be intercepted, if applicable;*

(f) *the nature and location of the place, if known, at which communications are to be intercepted;*

(g) *the number of instances, if any, on which an application has been made in relation to the same subject matter or the same person and whether that previous application was rejected or withdrawn;*

(h) *the period for which the authorisation is requested; and*

(i) *whether other less intrusive means have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or whether the matter is so urgent that less intrusive means cannot be tried.*

(G) Duration and renewal of warrant

6.11 A warrant should be issued for an initial period not exceeding 90 days and renewals may be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the initial application) to continue to be necessary.

6.12 An application for renewal of a warrant should be accompanied by an affidavit which includes the following matters:

(a) *the reason and period for which the renewal is required;*

(b) *particulars about the interceptions already made under the warrant and an indication of the nature of information obtained by such interceptions; and*

(c) *(i) the number of instances on which an application for renewal had been made in relation to the same warrant or the same target and whether the previous application was withdrawn, denied or approved, (ii) the date on which each application was made, and (iii) the name of the judge to whom each such application was made.*

(H) Entry on to premises to effect interceptions

6.13 An application for a warrant authorising interception of communications may include a request that the warrant authorise entry on to premises for the purposes of the interception but not otherwise.

(I) Content of warrant

6.14 The warrant authorising interception of communications should be specific as to -

(a) the object or objects of the proposed interception;
(b) the type of communications to be intercepted; and
(c) the method by which the communications are to be intercepted.

6.15 The authorising judge may impose such other restrictions or conditions as he may consider appropriate.

(J) Ex post facto applications

6.16 The court may issue a warrant ex post facto where there is reasonable cause to believe that -

(a) a warrant would have been granted if the making of an application prior to interception had not been rendered impracticable because of the urgency of the situation; and

(b) a pressing and imminent opportunity to secure information of a significant nature arises in circumstances where the urgency of the situation is such that an application for a warrant prior to interception would be likely to frustrate -

(i) the prevention of serious crime;

(ii) the apprehension of those reasonably suspected to be responsible for a serious crime; or

(iii) the obtaining of information which is likely to be of substantial value in safeguarding public security in respect of Hong Kong.

6.17 Where an interception is made without the authority of a warrant , an application for subsequent ratification should be made to the court within 48 hours after the decision to intercept has been made.

6.18 Where it is impracticable for the Administration or its law enforcement agency to obtain prior authorisation from the court because of the urgency of the situation, the officer proposing to make an interception

should, before initiating the interception, obtain authorisation from an officer at the directorate level who is designated for the purpose of giving authorisations in urgent situations.

6.19 Where the directorate officer reasonably believes that the criteria for the issue of a warrant are satisfied and the urgency of the situation necessitates the interception of communications before making an application to the court, he may, on such terms and conditions as he thinks fit, give authorisation to intercept a communication for a period not exceeding 48 hours.

6.20 An officer who proposes to make an interception without prior authorisation of the court should apply for permission from a directorate officer on every occasion he proposes to do the same. The permission to make an interception must be recorded in writing. Further, its terms and conditions must be specific.

6.21 In applying for a warrant ex post facto, the officer should serve on the court :

(a) an affidavit which includes particulars of the urgent situation because of which the applicant reasonably believed that it was impracticable for him to obtain prior authorisation from the court; and

(b) a copy of the authorisation given by a directorate officer authorising the interception of communications prior to making an application to the court.

6.22 Where an interception is made without the prior authorisation of the court, the interception should terminate as soon as the purpose is achieved or when the application is denied by the court, whichever is the earlier; and

6.23 Where the ex post facto application is denied by the court, the interception should be treated as unauthorised and the material obtained as a result of the interception should be destroyed immediately.

6.24 Where an ex post facto application is denied by a judge, the directorate officer authorising the interception of communications in an urgent situation, or the officer making an interception on authority of a directorate officer, should not be guilty of unlawful interception if the court is satisfied that the officer concerned acted in good faith when authorising or making the interception.

6.25 An application should be allowed to be made ex post facto to ratify an interception which was not covered by an existing warrant because of an honest error committed by the applicant, provided that -

(a) the application is made within 48 hours of the applicant having notice of the error; and

(b) the interception would have been authorised if the applicant had applied for it at the time he made the original application.

The application should be accompanied by an affidavit which includes the particulars of the error committed by the applicant and how and when the error was discovered.

The need for a warrant system

6.26 Two main approaches are possible in determining the scope of statutory exceptions:

a) stipulating that they are defences which can be invoked by the intercepting party if the party subject to the interception *subsequently* challenges the legality of the interception in court. This is the approach adopted under the Personal Data (Privacy) Ordinance (Cap. 486).

b) implementing a warrant system which requires the would-be interceptor to satisfy the issuing authority *before* the interception takes place that it falls within one of the specified exceptions. The authority's decision would be challengeable in court.

6.27 We consider that a warrant system is preferable:

a) where the authority cannot effect the intrusion without technical assistance (for instance, by the telecommunication service provider); or

b) where the activity in question is likely to be challenged, such as where there is physical entry to premises.

6.28 Under the Personal Data (Privacy) Ordinance the exception is invoked by the data user on the basis that the terms of the statutory exemption apply. This is subject to challenge by the data subject, and the matter will then be reviewed by a supervisory authority. While this system is appropriate to deal with departures from the data protection principles, we consider it inadequate in sanctioning the more serious intrusions entailed in the interception of communications. In addition, under the Personal Data (Privacy) Ordinance data subjects will become aware of refusals of access and any changes of use. An individual will seldom, however, become aware that he is the object of interceptions.

6.29 The alternative is a warrant system. This is the conventional mechanism adopted by, for instance, the United Kingdom legislation in sanctioning intrusions such as entry and search of premises and interception of communications. It has two advantages. Firstly, it entails approval by an independent authority before the intrusion is undertaken. Secondly, it furnishes the intruder with a written authority which he can produce if challenged. This second advantage is a practical necessity where the intrusion in question falls into one of the following categories:

(a) The intrusion requires the technical assistance of a third party. This is the usual position when intercepting communications carried by public telecommunications systems.

(b) The intrusion is of a nature which carries the risk of being detected by the victim. This is the case where physical intrusion into premises is involved.

6.30 We note that in the United Kingdom, intrusions regulated by law (and hence the warrant requirement) fall into one or other of these categories. The issue arises whether a warrant should also be required in those situations where the intrusion requires no external assistance and is inherently undetectable.

6.31 We have concluded that, in view of the seriousness of such intrusions, a warrant requirement should apply to all proscribed interception activities. To subject only some intrusions to the warrant procedure would encourage use of surveillance and interception activities that fell outside that requirement. As mentioned at the outset, we endorse an integrated approach to the regulation of intrusions for this reason.[1]

6.32 **We recommend that a warrant should be required to authorise all interceptions of communications falling within the scope of the proposed offence prohibiting these activities.**

The issuing authority

6.33 We note that in the United Kingdom it is a government Minister who authorises the warrant, whereas in the United States it is a court. In Australia, a court deals with law enforcement warrants and the Attorney General deals with security-related warrants.

6.34 Section 2 of the United Kingdom Interception of Communications Act 1985 confers on the Secretary of State a discretion to issue a warrant authorising an interception. Lustgarten and Leigh comment that this issue of warrants by a government minister, rather than a judge:

---

[1] The existence of a warrant system also protects the security agencies against pressures by others, particularly ministers, to operate improperly : Lustgarten and Leigh, *op cit,* at 411.

"may seem anomalous for several reasons: interception is analogous to search, for which warrants are issued by the judiciary (when required in law) and it offends conceptions of the rule of law and separation of powers for a minister of the crown to authorise interception by another part of the executive. It fails to provide an independent check on the power to prevent potential political abuse. While there may be a strong case for implementing the recommendation of the Royal Commission on Criminal Procedure that interception warrants should be issued by magistrates in criminal investigations, whether those arguments apply with equal force in the domain of security investigations is more doubtful. Certainly it may be said that the nature of the evidence supporting the application will be different in the two types of case. In these circumstances a minister may, because of access to background information, have a fuller picture than a magistrate or a judge of the overall intelligence significance of the proposed surveillance. ... In view of the fact that the process will of necessity exclude the targeted person from making representations prior to interception, it seems essential to require the authorities to satisfy an outsider of the need for it. We would, therefore, favour the introduction of a greater independent element (though not necessarily judicial control) prior to interception occurring."[2]

6.35 We consider that the additional independence afforded by a judicial determination is necessary in Hong Kong. We think that all warrants sanctioning intrusions should be authorised only by the courts, with no distinction made between warrants relating to law enforcement and those relating to public security in respect of Hong Kong. Distinguishing between warrants according to whether they relate to crime (for the judiciary) or public security (for the executive) would, we think, be difficult, with some circumstances falling into both categories. The aim of the system we propose is to strike a balance between the public interest and the rights of the individual. The judicial warrant system is designed to determine that balance when there is a conflict between the rights of the individual and the interests of the Administration. We think it essential for the maintenance of public confidence in the system that there is an independent review of the Administration's actions in this sensitive area. That would not be achieved by allowing high public officials to approve applications made by another part of the Administration; we believe it can best be achieved by introducing a judge as an independent arbiter of the necessity of an interception. Judicial involvement in the process will ensure that those applying for the warrant will have to think the matter through and diminish the prospect of abuse of power. Restricting the power to the High Court should also make for greater consistency of approach.

[2] Lustgarten and Leigh, *op cit,* at 55-56.

6.36 **We recommend that all applications for warrants for interception of communications should be made to a judge of the High Court.**

6.37 In view of the sensitive nature of interception activities, all applications would be made *ex parte*. As with other *ex parte* applications, a warrant application may be dealt with on paper but an oral hearing or an appearance before the judge may be required. By the nature of the application, the proceedings must be kept private.

6.38 If our proposals on the warrant system are adopted, section 33 of the Telecommunication Ordinance (Cap. 106) and section 13 of the Post Office Ordinance (Cap. 98) ought to be repealed. However, the power of the Post Office under section 13(2) of the Post Office Ordinance to delay a postal packet for the purpose of obtaining a warrant may be retained.

6.39 **We recommend that the Postmaster General should have a power to delay a postal packet for such time as may reasonably be necessary for the purpose of obtaining a warrant authorising him to intercept postal packets.**

6.40 None of the submissions received in response to the consultation paper objected to the setting up of a warrant system. The Bar Association agreed with the recommendations in the paper. The Law Society had no objection to regulating the legitimate interception of communications through the issuance of *ex parte* warrants.

6.41 One respondent was concerned that the decision of the judge would be based entirely on the evidence submitted by the applicant and that the persons whose communications were to be intercepted would not have any opportunity to challenge that evidence at the time of the application. We believe this concern will be met by our recommendation below that the applicant would be required to support his application by an affidavit or affidavits. The persons swearing the affidavits would render themselves liable to prosecution for perjury if they knowingly or recklessly gave false evidence on oath. Furthermore, we recommend later that the warrant system should be subject to monitoring.

Grounds on which a warrant may be issued

6.42 The freedom from interference with privacy is not absolute. It must be set against competing public interests, such as the suppression of crime. However, these limitations on the freedom must be necessary for the exercise of the competing interests and must be necessary in a society subject to the rule of law. We now examine the circumstances in which a warrant may be granted.

Prevention or detection of serious crime

6.43 Our guiding principle is that the means of investigation must be proportionate to the gravity of the matter under investigation. As interception of communications without the consent of the parties is a serious intrusion upon individual privacy, we believe that interception of communications for the purpose of investigating crime can be justified only if the offence under investigation is a serious one.

Prevention or detection

6.44 The provisions of the United Kingdom Interception of Communications Act 1985 extend to the "prevention or detection" of crime. The House of Lords held in *R v Preston*[3] that "the prevention or detection of crime" did *not* extend to the *prosecution* of the offence:

> "*To my mind the expression 'preventing and detecting' calls up only two stages of the fight against crime. First, the forestalling of potential crimes which have not yet been committed. Second, the seeking out of crimes, not so forestalled, which have already been committed. There, as it seems to me, the purpose comes to an end. I accept that the successful prosecution of one crime may in a sense prevent another, either because it puts the particular offender out of circulation for a while, or because the fact of conviction in respect of one crime may deter the commission of others. But although prevention in this sense may be a by-product of a prosecution, the word seems a very odd choice if the purpose of the interception was to reach forward right up to the moment of a verdict.*"[4]

6.45 The essential policy question is whether it is right that intrusions should be legally sanctioned only at the investigative stage.[5] We agree with the United Kingdom approach whereby intrusions should only be lawful up to the point when the formal prosecution process begins. That point would be determined as the laying of the charge. Such a restriction would accord with the present position whereby a suspect is not further interviewed once he has been charged and would also accord with legal professional privilege. However, additional warrants should be obtainable for intrusions to prevent or detect other crimes pertaining to an individual who has already been charged.

6.46 **We recommend that a ground for issuing a warrant authorising interception of communications should be that it is for the purpose of preventing or detecting serious crime.**

---

3 [1993] 4 All ER 638.

4 *Ibid,* at 666. The Court considered that this conclusion also accorded with the stringent limitations on the retention of intercepted data prescribed by section 6 of the UK 1985 Act (discussed in the next chapter).

5 The admissibility of materials obtained through interception is a separate issue considered in chapter 7.

Serious crime

6.47 The United Kingdom Act allows interception where it is for the purpose of "preventing or detecting serious crime". "Serious crime" is defined by section 10(3) of the Act as follows:

> "*(a) it involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or*
>
> *(b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more."*

6.48 The Bar Association is in favour of adopting this definition.

6.49 While the second limb in (b) above is definite enough, the first limb in (a) has been criticised for its vagueness. The National Council for Civil Liberties in the United Kingdom have the following comments:

> *"Not only are these categories unacceptably wide, they are also unacceptably vague. ... The drafting of this [provision] begs further questions: what amounts to 'substantial financial gain'? What would constitute 'a large number of persons'? The concept of 'common purpose' is a complex one. What standard of evidence would be required for a warrant to be issued in respect of people acting 'in pursuit of a common purpose'? Is it anticipated, for example, that people protesting peacefully on a public highway about live animal exports could be the subject of a ... warrant (they may technically be committing any number of common law or statutory offences, and they may be acting in pursuit of a common purpose)?"*[6]

6.50 The South African Act adopts a similar approach. "Serious offence" is defined as meaning any offence in Schedule 1 to the Criminal Procedure Act 1977 provided that -

> (i) it is being or has been committed over a lengthy period of time;
> (ii) it is being or has been committed on an organised basis;
> (iii) it is being or has been committed on a regular basis; or
> (iv) it may harm the economy of South Africa.[7]

---

[6] Liberty, *Briefing on the Security Service Bill 1996* (1996), p 8.

[7] Section 1.

6.51 We have reservations in adopting the United Kingdom approach. We think it undesirable that a judge be vested with a wide discretionary power over matters affecting an individual's right to communicate in private. It will be recalled that in *Malone* the European Court held that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances" in which interceptions will be authorised.

6.52 The comparable provision in the Australian Telecommunications (Interception) Act 1979 is more restrictive and specifies that the offence in question is punishable by 7 years imprisonment. It provides that an offence is a "class 2 offence" if -

> *"(a) it is an offence punishable by imprisonment for life or for a period, or maximum period, of at least 7 years; and*
>
> *(b) the particular conduct constituting the offence involved, involves or would involve, as the case requires:*
> *(i) loss of a person's life ...; or*
> *(ii) serious personal injury ...; or*
> *(iii) serious damage to property in circumstances endangering the safety of a person; or*
> *(iv) trafficking in prescribed substances; or*
> *(v) serious fraud; or*
> *(vi) serious loss to the revenue of the Commonwealth ...; or*
> *(vii) bribery or corruption ..."*[8]

An offence is also a "class 2 offence" if it is an offence involving planning and organisation, i.e. an offence punishable by imprisonment for life or for a period of 7 years where the offence (i) involves two or more offenders and substantial planning and organisation; (ii) involves the use of sophisticated methods and techniques; and (iii) is committed in conjunction with other like offences.[9]

6.53 As these provisions indicate, the difficulty is in identifying the cut-off point distinguishing "serious" crime from other crime. We note, however, that the United Kingdom provision does not refer to the maximum sentence, but to the tariff that is likely to be imposed in the particular case. This would usually be much less than the maximum prescribed.

6.54 The Hon James To invited us to consider the option of adopting a schedule of offences to define the concept of "serious crime," using the schedules to the Organized and Serious Crimes Ordinance (Cap. 455) as a

---

[8] Section 5D(2). A "class 1 offence" means a murder, a kidnapping or a narcotics offence: section 5(1). See Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (1994), section 2.3. Cf The Parliament of the Commonwealth of Australia, *Report of the Joint Select Committee on Telecommunications Interception* (Parliamentary Paper No 306/1986), chapter 4.

[9] Section 5D(3).

starting point.[10] This is the approach adopted in Canada and the United States. The Canadian Criminal Code and the United States Wiretap Act do not rely on the notion of "serious crime" or "serious offence". Instead, they list the offences which may form the basis of an application for an authorisation to intercept communications.[11] We are not in favour of this approach because of the need to ensure constant updating.

6.55 In its consultation paper, the sub-committee recommended that an offence punishable by a maximum sentence of at least 7 years imprisonment would adequately reflect the gravity of the offences which should justify the issue of a warrant. To reflect the fact that some offences which do not attract sentences at that level may nevertheless be considered by the community to pose such a threat to the fabric of society that they should fall within the scope of "serious crime" for the purposes of the warrant proposals, the sub-committee also recommended in the consultation paper that "serious crime" should include an offence punishable by a maximum sentence of at least 3 years imprisonment where there is an element of bribery or corruption.

6.56 The Bar Association objected to this recommendation on the ground that it was illogical and arbitrary to define "serious crime" by reference only to the maximum sentence, without regard to the circumstances of each individual case. We believe, however, that to define "serious crime" by virtue of the maximum sentence applicable to the offence achieves the necessary degree of certainty in the law, while avoiding the difficulties associated with providing a schedule of specific offences. Where the level of maximum sentence is pitched is, we think on further reflection, a matter for the Administration rather than this Commission. We have concluded, therefore, that while the maximum sentence should define what amounts to a "serious crime", we should not make any recommendation as to the appropriate length of that sentence. It may be that more than one level of sentence should be fixed so that, for instance, account can be taken of the proposal in the consultation paper that offences involving an element of bribery or corruption should qualify as "serious offences" at a lower sentencing threshold.

6.57 **We recommend that "serious crime" should be defined by virtue of the maximum sentence applicable to the offence. The appropriate level of sentence should be determined by the Administration, but account should be taken of the need to provide a lower sentencing threshold for offences involving an element of bribery or corruption.**

---

[10] We note that a person who is guilty of corrupt practice is liable to imprisonment for 7 years under the Corrupt and Practices Ordinance (Cap 288) but neither the schedule prepared by the Hon James To nor the 2 schedules in the Organized and Serious Crimes Ordinance incorporates such offences.

[11] Canadian Criminal Code, section 183; US Wiretap Act, section 2516.

Safeguarding public security in respect of Hong Kong

6.58 Matters relating to the "security, defence or international relations in respect of Hong Kong" are specifically excluded from investigation by the Commissioner for Administrative Complaints under the Commissioner for Administrative Complaints Ordinance (Cap. 397). A similar exemption was subsequently adopted in the Personal Data (Privacy) Ordinance (Cap. 486). The sub-committee's consultation paper recommended that a further ground for issuing a warrant authorising interception of communications should be that it is for the purpose of safeguarding the security, defence or international relations in respect of Hong Kong.

6.59 Although most respondents agreed with this proposal, some were concerned that such a formulation would give rise to abuses unless the constituent elements of "security", "defence" and "international relations" were defined in the legislation. One respondent voiced the concern that the Government may rely on this ground to intercept the communications of political organisations.

6.60 The Australian Security Intelligence Organisation Act 1979 gives a definition of "security" in the following terms:

> *"(a) the protection of [Australia] from:*
> *(i) espionage;*
> *(ii) sabotage;*
> *(iii) politically motivated violence;*
> *(iv) promotion of communal violence;*
> *(v) attacks on Australia's defence system;*
> *(vi) acts of foreign interference;*
> *whether directed from, or committed within, Australia or not; and*
>
> *(b) the carrying out of Australia's responsibilities to any foreign country in relation to any matter mentioned in any of the subparagraphs of paragraph (a)".*[12]

6.61 The Canadian Security Intelligence Service Act 1984 allows the granting of a warrant to enable the Security Service to investigate "a threat to the security of Canada". "Threats to the security of Canada" means:[13]

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada;
> (b) foreign influenced activities that are detrimental to the interests of Canada;
> (c) activities in support of the use of serious violence against persons or property for a political purpose; and

---

12 Section 4.
13 Sections 2 & 21.

(d) activities leading to the destruction or overthrow by violence of the constitutionally established system of government of Canada.

6.62 The United Kingdom Security Service Act 1989 makes no attempt to define the term "national security". However, it gives as examples "protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."[14]

6.63 We have noted the comments made on the consultation paper and have reservations as to the certainty with which the boundaries of "international relations" could be delineated. The interception of communications is a highly intrusive activity and we believe that the basis for making an application for a warrant should be tightly controlled. While an exception based on the term "international relations" may be satisfactory for restricting rights of redress under the Commissioner for Administrative Complaints Ordinance, we do not think it is precise enough to apply to the sensitive question of interception of communications. We note in addition that neither the International Covenant on Civil and Political Rights nor the Basic Law refer to "international relations".

6.64 We note that Article 30 of the Basic Law provides that the only ground on which a resident's privacy of communication may be infringed is "public security" or "investigation into criminal offences". The term "public security" is not defined, but we believe that it would be wide enough to cover defence and, in certain circumstances, international relations. Clearly, it is only sensible for our proposals to be in line with the Basic Law and we have therefore concluded that the recommendation in the consultation paper should be modified: instead of a reference to "security, defence or international relations", this ground for a warrant should be restricted to "public security" in respect of Hong Kong. **We recommend that a further ground for issuing a warrant authorising interception of communications should be that it is for the purpose of safeguarding public security in respect of Hong Kong.**

Safeguarding the economic well-being of Hong Kong

Article 8 of the European Convention on Human Rights

6.65 Article 8 of the European Convention provides that interference with an individual's private life and correspondence may be justified where it is necessary in the interests of the economic well-being of the country.

6.66 Alexandre Kiss explains that the limitation on the individual's right to privacy imposed by the phrase can be understood in the economic

[14] Section 2(1).

context in which the European Convention was drafted. The Convention reflected the foreign exchange regulations then common in Europe and the perceived necessity for opening correspondence to check currency violations.[15]

6.67 The term "economic well-being" is not used in the ICCPR. Even in the European Convention the phrase is used only in relation to the rights in article 8, but not other rights in the Convention. There is little jurisprudence in this area but the following European cases give us some idea as to the scope of the limitation permissible under the article.

(a) ***X v United Kingdom***[16] **:** In this case, the European Commission of Human Rights concluded that although a compulsory public census interfered with the right to respect for private life, it might be justified on the ground that it was in the interests of the economic well-being of the country because the object of such a census was usually to establish accurate statistical information about the population and the conditions of its housing.

(b) ***Wiggins v United Kingdom***[17] **:** The applicant was evicted under the housing control law in Guernsey from what had, until his wife left him, been his home. The law had been enacted to deal with the social and economic difficulties caused by an increasing population at that time. It provided that the occupation of all dwelling houses, with the exception of a small number of expensive dwellings, was to be subject to licence. The European Commission held that the law was pursuing the legitimate aim of preventing over-population harmful to Guernsey's economy and was therefore necessary for the economic well-being of Guernsey. The refusal of the Housing Authority to grant the applicant a licence to occupy his premises was justified on that ground, even though it interfered with his right to respect for his home.

(c) ***Funke v France***[18] **:** House searches and seizures may be carried out under the French Customs Code in order to prevent capital outflows and tax evasion. The relevant provisions aimed at protecting the stability of the currency and the equilibrium of foreign exchange transactions. The European Court of Human Rights noted that, in pursuing this aim, states encountered serious difficulties owing to the scale and complexity of banking systems and financial channels and to the numerous opportunities for international investment, made all the easier by the relative porousness of national borders. Recourse to measures such as house searches and seizures were therefore necessary in order to obtain physical evidence of exchange-control offences and, where appropriate, to prosecute those responsible. The

---

15 A C Kiss, *Permissible Limitations on Rights*, collected in : L Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (New York: Columbia University Press, 1981). at 290.

16 (1982) Appl no 9702/82, DR vol 30, p 239.

17 (1978) Appl no 7456/76, DR vol 13, p 40.

18 (1993) 16 EHRR 297.

Court concluded that the interferences in question were in the interests of the "economic well-being of the country".

6.68 These three cases show that the economic well-being ground is, in effect, open-ended. The danger is that it would enable Government officials or security agencies to define their powers and functions themselves. If the law enforcement agencies were vested with the power to intercept on this ground, there is a danger that the power might be abused.

United Kingdom

6.69 The Interception of Communications Act 1985 sanctions interceptions which are necessary "for the purpose of safeguarding the economic well-being of the United Kingdom".[19] This ground is in addition to that of "national security". During the second reading of the Bill, the Home Secretary stated that adverse developments overseas (such as a threat to the supply of a commodity such as oil on which the economy is particularly dependent) may have grave and damaging consequences for the country's economic well-being, even though they do not directly affect the national security.[20] He further explained how the provision would be implemented in practice:[21]

(a) The interception is not just desirable. It must be concerned with safeguarding the country's economic well-being and not with promoting it. That means it must be protective and relate to threats to the economic well-being.

(b) The matter must be one of national significance and cannot be of a trivial kind which is peripheral to the country's economic well-being.

(c) The purpose of the interception must be purely external. The information to be acquired must relate to the acts or intentions of persons outside the country.[22] Purely domestic events cannot give rise to the issue of a warrant on this ground.

6.70 The restriction in (c) above does not apply to the exception in article 8 of the European Convention. It is included in the statute so that industrial action and other internal economic disputes can be excluded under this head. It indicates that the matter under investigation relates to foreign affairs and not to the domestic affairs of the country.[23]

---

19 Section 2(2)(c).

20 75 *House of Commons Official Report*, col 159 & 160 (12 March 1985).

21 *Idem.*

22 Section 2(4).

23 The Security Service Act 1989 also specifies that one of the functions of the Security Service is to "safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands" : section 1(2) & (3). See 145 *House of Commons Official Report*, col 220 & 221 (17 January 1989). Section 2(2)(b) of the Act expressly requires the Service not to take any action to further the interests of any political party.

6.71 The wording of the relevant provisions in the Intelligence Services Act 1994 Act is broader than the 1985 Act. It omits the word "safeguarding" and simply provides that the Intelligence Service may exercise its functions "in the interests of the economic well-being of the United Kingdom". This is probably due to the fact that the purposes of the Intelligence Service are not confined to threats to the nation but include the furthering and promotion of the national interest. The Government explained that the following are matters with which the Intelligence Service would be concerned under this head:[24]

(a) the price and availability of commodities;
(b) financial and monetary policies of countries that might have an impact on the United Kingdom;
(c) activities of individuals abroad that might discredit financial institutions in the United Kingdom; and
(d) the promotion of British economic interests abroad.

Canada, Australia and New Zealand

6.72 There are no equivalent provisions in Canada. The definition of "threats to security of Canada" in the Canadian Security Intelligence Service Act 1984 does not expressly refer to economic matters. However, the legislation provides that the Service may, in relation to defence or the conduct of international affairs of Canada, assist the Minister "in the collection of information or intelligence relating to the capabilities, intentions or activities" of any foreign state or alien.[25]

6.73 Similarly, the term "security" in the Australian Security Intelligence Organisation Act 1979 does not mention economic matters. There have been reports, however, that the Organisation has an interest in the economic communications of certain foreign bodies.[26]

6.74 Recently, the New Zealand Government introduced a bill which proposed to amend the definition of "security" in the New Zealand Security Intelligence Service Act 1969[27] by extending its meaning to include "the ensuring of New Zealand's international well-being or economic well-being". No guidance is given in the Bill as to the exact meaning of that phrase. The Privacy Commissioner of New Zealand commented that the uncertainty in the phrase, and the possible interpretations which might be placed upon it, make it "a potentially dangerous step in relation to individual liberties to take". He said that

---

24 75 *House of Commons Official Report*, col 303 (27 April 1994). The Minister declined to comment on the allegation that "[the Government] have developed a habit of spying on foreign companies that compete with British companies, and rewarding British companies with titbits of information picked up through [Government Communications Headquarters] or elsewhere in return for unspecified favours."

25 Section 16.

26 L Lustgarten & I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994), at 393.

27 The Act defines "security" as meaning "the protection of New Zealand from acts of espionage, sabotage, terrorism and subversion, whether or not it is directed from or intended to be committed within New Zealand".

"any extensions must be made cautiously and in full knowledge of the new tasks that society is intending to ask its intelligence agencies to take".[28]

The economic interests requiring protection

6.75 The wording of the phrase in the United Kingdom Interception of Communications Act 1985 is broad enough to cover the communications of multinational enterprises, currency speculators and the diplomatic communications of Britain's partners in the European Union. Schweizer argues that with the end of the cold war, secret services are increasingly involved in industrial espionage. He quotes a former director of the French secret service:

> "*Spying in the proper sense is becoming increasingly focused on business and the economy, science and industry - and very profitable it is. It enables the Intelligence Services to discover a process used in another country, which might have taken years and possibly millions of francs to invent or perfect. This form of espionage prevails not only with the enemy but to some extent among friends ... . In any Intelligence Service worthy of the name you would easily come across cases where the whole year's budget has been paid for in full by a single operation. Naturally, Intelligence does not receive actual payment, but the country's industry profits."*[29]

6.76 Schweizer contends that such espionage is conducted by clandestine means. Business executives and trade negotiators are bugged and tracked at home and abroad. Corporate telecommunications are regularly monitored and intercepted.

6.77 Whilst the protection of traditional state secrets such as advanced military technology might be justified on the ground of national security, the protection of private interests in a competitive market is a different matter. It can be argued that the power of the state should not be invoked unless the interests requiring protection are serious enough to affect the country as a whole. The state should not intervene to protect interests only of a particular company or a particular sector of the economy. We note that the concept of a "local company" has become uncertain in the age of multi-national enterprises where labour and capital can move freely across national borders.[30]

6.78 The state might have a role in securing the supply of essential commodities at the most favourable price where the Government is the sole or main supplier of such commodities to the public. We note that some governments negotiate contracts on behalf of a major sector of the economy

---

28 B H Slane, *Report by the Privacy Commissioner to the Minister of Justice on the Intelligence and Security Agencies Bill*, (Auckland, 1996).

29 P Schweizer, *Friendly Spies* (1993), at 13.

30 See generally, Lustgarten & Leigh, *op cit*, at 27-30 and 390-394.

such as farmers. However, this argument has no application to Hong Kong. Hong Kong has a market economy, rather than a centrally planned economy, and government intervention in economic matters is minimal.

6.79 We believe that it is both legitimate and desirable for the Government to seek to maintain the economic stability and prosperity of Hong Kong. But we do not think that this can rightly be categorised as a matter of such gravity as to justify the invasion of privacy of citizens who are engaging in lawful commercial activities whether within or outside Hong Kong. The potential for abuse in our view outweighs the benefits that may accrue to society. A broad provision along the lines of the United Kingdom legislation is therefore inappropriate for Hong Kong, even if it were restricted to threats coming from overseas which affect the economic interests of Hong Kong as a whole.

The need to safeguard the stability of the local financial system

6.80 We turn now to consider whether a conspiracy to attack the financial system of Hong Kong might be an exception. The sub-committee was initially concerned that there may be hostile foreign actions or adverse developments overseas which do not necessarily amount to a threat to the security of Hong Kong so as to justify interception on that ground but may nevertheless have grave and damaging consequences for the financial system of Hong Kong. The consultation paper suggested that the importance of protecting the Hong Kong currency peg to the United States dollar merited special consideration. For example, a foreign investor or representatives of foreign governments may cause a run on the Hong Kong dollar sufficient to undermine the stability of the local financial system. The European case of *Funke* highlighted the complexity of the banking system and the relative porousness of national borders which make an attack on the local financial system from overseas all the easier and, at the same time, render any action to prevent or investigate such attacks more difficult.

6.81 The sub-committee also noted that article 8 of the European Convention acknowledges that the economic well-being of the country is a legitimate area for state concern, justifying some interference with the individual's right to privacy. The United Kingdom legislation contains provisions safeguarding the economic well-being of the country against threats from aboard, and there is nothing to suggest that foreign investment has been adversely affected by the existence of such provisions.

6.82 The consultation paper therefore recommended that one of the grounds for issuing a warrant should be that it is for the purpose of safeguarding the stability of the local financial system. This recommendation extended to intrusions conducted both within and outside Hong Kong.

6.83 The overwhelming majority of those responding to the consultation paper objected to this proposal. Their arguments included the following:

(a) The proposal would interfere with the free market and would undermine Hong Kong's status as an international financial centre.

(b) Although currency speculation may be immoral, it is not a crime nor should it be if Hong Kong is to retain its role as an international financial centre.

(c) Support for the concept of the currency peg is not universal.

(d) Economic issues should be addressed by economic measures. Similarly, the stability of the financial system should be safeguarded by financial means.

(e) The protection of the financial system is a matter for the Hong Kong Monetary Authority. The Exchange Fund is a far more potent weapon with which to defend the local currency.

(f) There would be a risk that bankers, economists and journalists might be prosecuted for discussing and soliciting economic data.

(g) Businesses would move to other cities.

6.84 Before coming to our conclusion, we wish to make a comment on item (f) above. To suggest that there is a risk of prosecution for discussing and soliciting economic data if interceptions are to be authorised on the grounds of protecting the territory's economic well-being is to misrepresent the case. The consultation paper did not propose that conduct which is not at present criminal should be so rendered. Rather, it proposed a specific set of circumstances in which application may be made for a warrant to intercept communications. The nature of the communications themselves would not change: if they are criminal now, they would remain so; if they are not, the consultation paper's recommendation would not change that.

6.85 Nonetheless, we are persuaded on balance of the validity of the case put forward by those who argued against special treatment for the currency peg. We are particularly impressed by the argument that currency speculation is not a crime. If there were truly a mischief in existence which ought to be proscribed, it is a matter for the legislature to make it a criminal offence. In our opinion, it is only when the threat to the local economic and financial system impinges on the public security of Hong Kong that the law enforcement agencies should have a power to intrude upon an individual's privacy. Given that the Hong Kong Monetary Authority did not support the recommendation in the consultation paper, it is difficult to argue that there is a need to intercept communications for the purposes of safeguarding the stability of the local financial system.

6.86 We conclude that neither the stability of the local financial system nor the economic well-being of Hong Kong is a matter of such gravity as to justify the issue of warrants for the interception of communications unless the threat to the financial system or economic well-being impinges on the public security of Hong Kong.

General defence of public interest

6.87 A few respondents suggested that there should be a public interest defence.[31] The Hon James To proposed that the defence should be available to an accused who intercepted a communication in good faith and clearly in the public interest. The Hong Kong Journalists Association believed that this defence was necessary to prevent the proposed legislation being applied in an oppressive manner.[32]

6.88 In the United Kingdom, neither the Calcutt Committee nor the Younger Committee found it desirable to create a general defence of public interest. The Younger Committee commented:

> *"a court would in effect have to make an unguided choice, in the light of the public interest, between values which, in the abstract, might appear to have equal weight. We recognise that the courts could be given the task of considering, in the factual context of each case, whether a general right to privacy should be upheld against the claims of other values, in particular the value of the free circulation of true information. But we think that such a task might first make the law uncertain, at least for some time until the necessary range of precedents covering a wide range of situations had been established; and it might secondly extend the judicial role, as it is generally understood in our society, too far into the determination of controversial questions of a social and political character."*[33]

6.89 None of the overseas laws we examined provide for an exemption on the ground that the interception was executed in the public interest. In most other jurisdictions, interception of communications is authorised only if the information obtained as a result of the interception would assist in the investigation of a crime or a threat to security.

6.90 We are not in favour of adopting a general defence of public interest. The public interests requiring exemption should be identified and specified in the legislation. Article 30 of the Basic Law expressly provides that

---

31 As to the argument that interception should be permissible if the publication of the intercepted information is in the public interest, see chapter 9 below.

32 The Hong Kong Journalists Association accepted that a wiretap by a journalist is unethical and it knew of no case in which a media organisation had intercepted communications in such a way that would contravene the law if our recommendations were adopted, with the exception of intercepting "unencrypted radio transmissions which are widely known to be insecure by their users".

33 *Report of the Committee on Privacy* (Cmnd 5012, 1972), paragraph 653.

the privacy of communications should not be infringed except "to meet the needs of public security or of investigation into criminal offences". We conclude that prevention or detection of serious crime and safeguarding public security in respect of Hong Kong are the only public interests justifying the interception of communications. In any event, since we shall recommend below that only the Administration and its law enforcement agencies should be entitled to apply for a warrant and since it would be an offence only if the interception was carried out intentionally, the issue of public interest would not arise in practice.

Application by the private sector

6.91 In other jurisdictions the warrant system envisages the approval only of intrusions carried out by public authorities. In principle, however, it can be argued that a private citizen should have a right to obtain a warrant if he is able to show that the intrusion can be justified on one of the grounds specified in the legislation.

6.92 For example, a company may suspect that there is criminal activity within its organisation but may have an insufficient basis for that belief to justify making a report to a law enforcement agency. Even if there is some evidence, the company may want to collect more information before approaching the authorities. Companies that wish to avoid the embarrassment of a police investigation may hire private investigators to investigate offences. Enabling the private sector to apply for warrants to intercept communications may, in rare cases, facilitate the exposure of illegal activities acquiesced in, or sanctioned by, the public authorities.

6.93 In addition, there may be instances where a private person (e.g. the media) would like to investigate a matter which is of a serious nature and affects the public good, but does not necessarily amount to a serious crime. Examples are breaches of the Listing Rules under the Securities Ordinance (Cap. 333) and situations where a public officer is putting himself in a position where there is a conflict of interests.

6.94 In the United Kingdom, the Calcutt Committee proposed that physical intrusion into private premises may be justified on the following grounds: (a) preventing, detecting or exposing the commission of any crime, or other seriously anti-social conduct; and (b) protection of public health or safety.

6.95 In view of these observations, the consultation paper recommended that authorisation by warrant should be available to sanction intrusions by both the public and the private sectors. We have revised that preliminary view in the light of the submissions made to the sub-committee.

6.96 The Hon James To made the following comments:

"We are sceptical about allowing private companies to use such intrusive methods as wire-tapping because unlike police officers, private companies are not subject to any licensing regulations or disciplinary code or to any scrutiny by bodies such as the Legislative Council. It would be unwise therefore to give them these intrusive powers devoid of any accountability."[34]

6.97 It can be argued in reply that the fact that private companies are not subject to any licensing regulations or disciplinary measures only highlights the need for private sector intrusions to be authorised by and under the control of the court. Subjecting the private sector to the warrant system would ensure that private investigators would act within the confines of a legislative framework. It would also make them accountable for their intrusive actions.

6.98 Nevertheless, we have concluded that the right to apply for a warrant should be restricted to the Administration and its law enforcement agencies. We think it desirable that any person who detects or suspects that there is a crime should report the matter to the police rather than pursuing a private investigation of their own. Moreover, if the private sector were allowed to intercept private communications, it would be extremely difficult to control the subsequent use and disclosure of information obtained by the interception. There is always the risk that material which relates to the private life of an individual is released to the media for public disclosure. The creation of criminal offences to prohibit unauthorised use and disclosure of intercepted material may not be the most effective way to prevent such conduct. We believe that the potential for abuse outweighs any advantage which might be expected to flow from allowing the private sector to apply for warrants to intercept.

6.99 Furthermore, none of the examples quoted above are matters of a gravity comparable to that of serious crime. We believe it is reasonable for the public to expect that their telephone conversations would not be intercepted unless they are perpetrating or conspiring to commit a serious crime. We conclude that there are no other public interests which are of sufficient gravity to justify the interception of communications by the private sector.

6.100 In a society subject to the rule of law, the power to intercept private communications should lie solely in the hands of the Administration. The Administration is entrusted with responsibilities to maintain law and order and is accountable to the public. The checks and balances in our system ensure that the Administration performs its functions within the confines of the law. In contrast, there is no guarantee that the authority to intercept granted by the court would not be abused if the interceptor is an individual or a private organisation.

---

[34] Position Paper on "Privacy: Regulating Surveillance and the Interception of Communications" submitted by the Office of the Hon James To Kun-Sun, 19 June 1996.

6.101 While there may be activities which ought to be exposed and censured even though they do not amount to a serious crime, or any crime at all, this does not in our view justify the private sector using intrusive methods such as the interception of communications to uncover such immoral or reprehensible conduct. If the conduct in question is of such a serious nature that it ought to be proscribed, then it is a matter for the legislature to consider whether it should be rendered a criminal offence, thereby bringing in the investigative power of the law enforcement agencies.

6.102 **We recommend that only the Administration and its law enforcement agencies may apply for a warrant authorising interception of communications. The application should be made by a senior officer but it should be a matter for the Administration to decide which of its post-holders should be authorised to apply for warrants.**

Form of application

6.103 The Hong Kong Alliance of Chinese and Expatriates submitted that some form of informal authorisation should be allowed in cases of emergency. They cited the examples of telephone application and the making of an "informal deposition" pending proper documentation.

6.104 In Australia, the chief officer of a law enforcement agency may make an application by telephone in urgent circumstances if he thinks that this is necessary. The application should provide particulars of the urgent circumstances and such information as would have been required if the application had been made in writing. The person who gives such information to the judge is required to swear an affidavit setting out the information so given by him within one day after the day on which a warrant is issued on the telephone application.[35]

6.105 We hold the view that the applicant should always apply in writing. Although a person who makes a telephone application may be required to provide the judge with the same information which would have been required if the application had been made in writing, it is highly unlikely that he would have the time to do so if there is truly an emergency. Furthermore, our proposals will allow a person to make an application *ex post facto* if the making of an application was impracticable because of the urgency of the situation. It is therefore not necessary to make provision for telephone applications.

6.106 **We recommend that an application for a warrant authorising interception of communications should be made in writing.**

[35] Telecommunications (Interception) Act 1979 (Australia), sections 40, 43, 50, 51, 52 & 58.

Matters on which judge must be satisfied

General principles

6.107 The following principles governing intrusion were formulated by the Canadian Royal Commission on the secret services:[36]

(a) the rule of law is paramount;

(b) the means of investigation must be proportionate to the gravity of the threat;

(c) the need for investigative techniques must be weighed against the damage they might do to personal freedom and privacy;

(d) the more intrusive the technique, the higher the authority should be to authorise its use;

(e) except in emergencies, less intrusive techniques must be preferred to more intrusive ones.

6.108 We agree that the judge should take these principles into account in granting an order authorising interceptions. He should balance the competing interests of the public with the individual's right to freedom from privacy invasion. He should bear in mind the privacy implications not only on the target but also on others who may be affected unintentionally by the authorised intrusion. Regard should be had to the fact that the longer the duration of a warrant, the more likely that personal information which is not relevant to an investigation would be acquired or captured.

6.109 In addition, the means of investigation should be proportionate to the immediacy and gravity of the alleged crime. Other things being equal, less intrusive techniques should be preferred to more intrusive ones. The purpose of the proposed intrusion is also relevant. It should be expected that the judge would impose more stringent controls if the law enforcement agency merely wants to gather intelligence.

6.110 Many jurisdictions impose additional requirements before a warrant can be issued. The two principal restrictions are that there is reasonable suspicion and the information cannot reasonably be acquired by less intrusive means. These requirements will now be examined.

---

[36] Commission of Enquiry into Certain Actions of the Royal Canadian Mounted Police, *Freedom and Security under the Law*, (Ottawa, 1981), at paragraph 411.

Reasonable suspicion

6.111 In the United States, the judge may enter an order authorising interception if he determines on the basis of the facts submitted by the applicant that:

> *"(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;*
>
> *(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; ...*
>
> *(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."*[37]

6.112 Similarly, under the German law "exploratory" interceptions are not permitted. An order to intercept communications "may be directed only against the suspect or against persons who on the basis of specific facts may be assumed to receive or convey information addressed to the suspect or originating from him".[38]

6.113 In *Malone*, the United Kingdom told the European Court that "likelihood of conviction" was applied as a requirement. Despite the White Paper's endorsement of this requirement,[39] it was subsequently omitted from the 1985 Act. Halsbury opines that it is nonetheless a precondition.[40]

6.114 We agree that interceptions should be lawful only in relation to individuals who are reasonably suspected of committing a serious crime. In addition, the applicant should reasonably believe that information relevant to the investigation will be obtained through such interceptions. Intrusive techniques should not be used for fishing expeditions. This is particularly so in view of the new technologies that facilitate telephone tapping through means such as key word recognition.

---

37 Wiretap Act, section 2518(3). The requirements of subsection (3)(d) relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if, in the case of an application with respect to an oral communication, the judge finds that such specification is not practical; or, in the case of an application with respect to a wire or electronic communication, the judge finds that the target intends to thwart interception by changing facilities: section 2518(11).

38 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications, section 2(2).

39 *The Interception of Communications in the United Kingdom* (Cmnd 9438, 1985), para 20.

40 *Halsbury's Statutes*, vol 45, at 419.

6.115 The requirement of reasonable suspicion is less appropriate in the context of security than it is for crimes. Hence the United Kingdom Security Service Act 1989 provides that the intrusion must be thought:

> *"necessary for the action to be taken in order to obtain information which (i) is likely to be of substantial value in assisting the Service to discharge any of its functions; and (ii) cannot reasonably be obtained by other means".*[41]

6.116 We agree that a similar restriction should be imposed on interceptions for the purposes of safeguarding public security in respect of Hong Kong. Interceptions should only be permitted where the information to be obtained through the interception is likely to be of substantial value in safeguarding public security in respect of Hong Kong.

Information that cannot reasonably be acquired by less intrusive means

6.117 The United Kingdom Interception of Communications Act 1985 provides that in determining whether a warrant is justified, a relevant matter is whether the information "could reasonably be acquired by other means".[42] The United States Wiretap Act is more explicit and requires the judge to be satisfied that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous".[43]

6.118 The German and Canadian laws have similar provisions. The former requires that other investigatory methods would be ineffective or considerably more difficult.[44] The latter requires that:

> *"other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."*[45]

6.119 We endorse this restriction that interceptions should not be authorised unless the information is not reasonably available by less intrusive means. These other overt means will generally be more difficult so that the test must not only relate to the relative ease of deploying intrusive techniques, but the *reasonableness* of so doing. This test would balance efficiency with the competing public interest in providing protection from intrusion.

---

41 Section 3(2)(a). Section 5(2)(a) of the UK Intelligence Services Act 1994 contains similar provisions.

42 Section 2(3).

43 Wiretap Act, section 2518(3)(c).

44 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications, section 2(2).

45 Criminal Code, section 186(1)(b).

6.120 **We recommend that a warrant authorising interception of communications should be issued only if the judge is satisfied that -**

(a) there is reasonable suspicion that an individual is committing, has committed or is about to commit a serious crime, or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong;

(b) there is reasonable belief that information relevant to the investigation will be obtained through the interception; and

(c) the information to be obtained cannot reasonably be obtained by less intrusive means.

6.121 **We recommend that in reaching a conclusion on the appropriateness of issuing a warrant, the judge should have regard to the following factors:**

(a) the immediacy and gravity of the crime or the threat to public security in respect of Hong Kong, as the case may be;

(b) the likelihood of the crime or threat occurring; and

(c) the likelihood of obtaining relevant information by the proposed interception.

Information to be provided on application for a warrant

6.122 In order to enable the court to make an informed decision as to whether or not to make an order, the applicant should provide the court with information showing that interception is necessary for the intended purpose.

6.123 The United States Wiretap Act requires "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[46] We support a similar provision requiring the applicant to provide details of the difficulties which would have arisen if the investigation were restricted to conventional methods.

6.124 **We recommend that an application for a warrant authorising interception of communications should be accompanied by an affidavit. The information to be provided in the affidavit should include:**

---

[46] Section 2518(1)(c).

(a) the name, identity card number and rank or post of the person making the application;

(b) the facts relied upon to justify the belief that a warrant should be issued, including the particulars of the serious crime or the threat to public security in respect of Hong Kong;

(c) the identity of the person, if known, whose communications are to be intercepted;

(d) a general description of the form of communications to be intercepted and the manner of interception proposed to be used;

(e) the nature and location of the facilities from which the communication is to be intercepted, if applicable;

(f) the nature and location of the place, if known, at which communications are to be intercepted;

(g) the number of instances, if any, on which an application has been made in relation to the same subject matter or the same person and whether that previous application was rejected or withdrawn;

(h) the period for which the authorisation is requested; and

(i) whether other less intrusive means have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or whether the matter is so urgent that less intrusive means cannot be tried.

Duration and renewal of warrants

6.125 Having determined the matters that must be made out to justify the issue of a warrant, the question of the warrant's duration requires consideration. We recommended in the consultation paper that a warrant should be issued for an initial period of 60 days. The Bar Association agreed that the period should be no longer than that. The Hon James To proposed that the period should be not more than 30 days so as to reflect the principle that interception is a last resort and should not be used unless it is absolutely necessary. Two other respondents commented that 60 days is too short and would like to see the duration extended to six months. Their concern is that investigations are often protracted and applying to court for renewal every two months would create inconvenience to the law enforcement agencies.

6.126 We are conscious that any decision on the length of warrant must be arbitrary. But the length is less of an issue than the arguments put forward by the applicant. If the applicant has a strong case, he can always come back to the court and apply for renewal. Nonetheless, we are concerned that the court might be burdened with unnecessary applications for renewal if the duration is as short as, say, 30 days.

6.127 We conclude that 90 days should suffice for both crime and public security. A similar period should govern extensions. In coming to this conclusion, we have considered the experience overseas. The position in other jurisdictions is summarised as follows:

(a) *Australia*
- 90 days if a criminal offence is involved;[47]
- Six months if the activities concerned are prejudicial to security.[48]

(b) *Canada*
- 60 days under the Criminal Code;[49]
- 60 days or 1 year under the Canadian Security Intelligence Service Act 1984.[50]

(c) *Germany*
- Three months.[51]

(d) *New Zealand*
- 30 days for investigation of organised crime.[52]

(e) *South Africa*
- 90 days.[53]

(f) *United Kingdom*
- 60 days under the Interception of Communications Act 1985;[54]
- Six months under the Security Service Act 1989[55] and the Intelligence Services Act 1994.[56]

(g) *United States*
- 30 days.[57]

---

47 Telecommunications (Interception) Act 1979 (Australia), section 49(3).

48 Telecommunications (Interception) Act 1979 (Australia), section 9(5).

49 Section 186(4)(e).

50 Section 21(5).

51 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications 1968, section 5(3).

52 Crimes Act 1961, section 312D(3).

53 Interception and Monitoring Prohibition Act 1992, section 3(3).

54 Section 4. It provides that warrants shall be issued for an initial period of 2 months and thereafter require renewal, also for a period of 2 months (but with provision for 6 months). Renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2.

55 Section 3(4).

56 Section 6(2).

6.128 We have considered adoption of an upper limit to the number of extensions given, but have rejected this because each extension would have to be justified on the prescribed criteria.

6.129 **We recommend that a warrant should be issued for an initial period not exceeding 90 days and that renewals may be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the initial application) to continue to be necessary.**

6.130 As the application is *ex parte*, it would be necessary that the applicant presents the court with all the material matters, including the history of all applications for renewal pertaining to the same warrant or the same target.[58]

6.131 **We recommend that an application for renewal of a warrant should be accompanied by an affidavit which includes the following matters:**

(a) the reason and period for which the renewal is required;

(b) particulars about the interceptions already made under the warrant and an indication of the nature of information obtained by such interceptions; and

(c) (i) the number of instances on which an application for renewal had been made in relation to the same warrant or the same target and whether the previous application was withdrawn, denied or approved, (ii) the date on which each application was made, and (iii) the name of the judge to whom each such application was made.

Entry on to premises to effect interceptions

6.132 The execution of a warrant may necessitate entry on to private premises. In the absence of a power to enter on to private premises, the applicant would have to apply for a separate warrant under existing legislation authorising him to enter the target premises.[59] We think it would be undesirable if the applicant has to apply to two different authorities for two separate warrants in order to effect a lawful interception which requires access to private premises.

6.133 **We recommend that an application for a warrant authorising interception of communications may include a request that**

---

57 Wiretap Act, section 2518(5).

58 Cf. Canadian Criminal Code, section 186(6).

59 E.g. Police Force Ordinance (Cap 232), section 50(7).

the warrant authorise entry on to premises for the purposes of the interception but not otherwise.

Content of warrant

6.134 As no interception can take place except under the authority of a warrant,[60] the warrant must be specific as to what the applicant can do. Furthermore, the judge should have a power to impose such conditions as he may consider to be appropriate.[61]

6.135 **We recommend that the warrant authorising interception of communications should be specific as to -**

(a) the object or objects of the proposed interception;
(b) the type of communications to be intercepted; and
(c) the method by which the communications are to be intercepted.

6.136 **We recommend that the authorising judge may impose such other restrictions or conditions as he may consider appropriate.**

Security of applications

6.137 One respondent commented that the handling of applications and the management of files by the court may give rise to problems in maintaining the confidentiality of information obtained through lawful interception.

6.138 We agree that the court should ensure that all documents relating to applications for warrants be kept in safe custody. It is essential that such documents (including the warrants themselves) are kept confidential. The whole system would be undermined if any information concerning the applications is divulged to the public. However, given that the court is experienced in handling confidential documents, we are confident that the court should have no difficulties in maintaining the secrecy of the application process. Whereas negligent disclosure by the staff of the court is a matter of internal discipline and procedure, a deliberate breach of security of a warrant could amount to a conspiracy to pervert the course of justice.

6.139 We conclude that it is not necessary for us to specify the manner in which documents relating to warrant applications are to be kept because this is a matter which falls within the purview of the Judiciary.

---

[60] Unless it falls within one of the recognised exceptions.
[61] Cf Canadian Criminal Code, section 186(4).

Ex post facto applications

6.140 Some respondents were concerned that the warrant system would adversely affect the operational efficiency of law enforcement agencies. We are satisfied that this concern is adequately met by the duty judge system which provides an applicant with 24 hour access to a High Court judge to consider his application. We recognise that there are emergency cases where it is impracticable to apply to a judge before initiating an interception. We think that interceptions in such situations should be subsequently ratified by judicial authorisation. Dispensing with a system of *ex post facto* authorisation could seriously undermine the safeguard of judicial scrutiny. The consultation paper therefore recommended that in circumstances where it is impracticable because of the urgency of the situation (as where life is at risk) to obtain approval from the court before initiating an interception, it should be permissible to apply to the court *ex post facto* for a warrant.

6.141 Only one respondent objected to the idea of allowing a person to apply for retrospective judicial authorisation - a concern we have addressed above.[62] The other respondents were generally supportive of our proposal.

6.142 The Hon James To suggested that there should be "a serious threat of death or bodily harm" before the provision on *ex post facto* warrants could be invoked. He commented that situations where damage to property would have serious implications should also be included.[63] We consider the condition must be wider than that suggested by the Hon James To because some offences which do not involve any serious harm to any person or property may nevertheless fall within our definition of serious crime. Corruption is a good example.

6.143 A law enforcement agency may receive intelligence that information which is likely to be of value to the prevention or detection of serious crime may be disclosed in communications shortly to be made. The agency should have been able to obtain a warrant under such circumstances if time permits them to do so. But if the urgency of the situation is such that it is impracticable for them to apply for a warrant before initiating an interception *and* the case under investigation does not involve any life-threatening situations, it would be impossible for the agency to apply for a warrant *ex post facto* under the original proposal even though it involves serious crime. If that were the case, the agency would have no authority to intercept the communications and a golden opportunity to gather crucial information might be missed.

---

62 The Hong Kong Alliance of Chinese and Expatriates commented that the person proposing to intercept a communication should apply to the court even in emergency situations although "some form of informal authorisation might be allowed on the basis of telephoned requests or informal deposition pending for the proper documentation". This comment was considered in the paragraphs under the heading of "Form of application" above.

63 He quoted the example of damage to the computer system of the Hong Kong Stock Exchange.

6.144 One respondent suggested that an *ex post facto* warrant should be issued "when a pressing and imminent opportunity to secure evidence or information of a significant nature arises in circumstances where the making of an application for a warrant may seriously impede the investigation into a suspected serious offence." We think that the determining factor should be the urgency of the situation which renders the making of an application impractical.

6.145 **We recommend that the court may issue a warrant *ex post facto* where there is reasonable cause to believe that -**

(a) a warrant would have been granted if the making of an application prior to interception had not been rendered impracticable because of the urgency of the situation; and

(b) a pressing and imminent opportunity to secure information of a significant nature arises in circumstances where the urgency of the situation is such that an application for a warrant prior to interception would be likely to frustrate -

(i) the prevention of serious crime;

(ii) the apprehension of those reasonably suspected to be responsible for a serious crime; or

(iii) the obtaining of information which is likely to be of substantial value in safeguarding public security in respect of Hong Kong.

6.146 **We recommend that where an interception is made without the authority of a warrant, an application for subsequent ratification should be made to the court within 48 hours after the decision to intercept has been made.** Thus, even though the interception may have terminated within 48 hours, the applicant would still be under an obligation to obtain authorisation from the court. Failure to do so would render him liable to prosecution; on the basis that all interceptions conducted in urgency should be subject to the scrutiny of the court shortly after the event.

6.147 One respondent suggested that the applicant should be required to obtain permission from the head of the law enforcement agency before conducting an interception. We agree that additional protection is needed to eliminate the possibility of an interception being made by a rogue officer. However, permission need not come from the head of the agency himself. Instead, he should be allowed to delegate the power to a small number of senior officers designated for such purposes. We consider that the authorising officers should be restricted to officers at the directorate level.

6.148 We believe that the authorisation of an officer at the rank of Assistant Director or above is required if the applicant is making an

application on behalf of the Independent Commission Against Corruption. In the case of the Royal Hong Kong Police Force, we think that the authorisation of an officer at the rank of Assistant Commissioner of Police or above would be more appropriate.

6.149 **We recommend that where it is impracticable for the Administration or its law enforcement agency to obtain prior authorisation from the court because of the urgency of the situation, the officer proposing to make an interception should, before initiating the interception, obtain authorisation from an officer at the directorate level who is designated for the purpose of giving authorisations in urgent situations**.

6.150 As we have recommended that an application to a judge must be made within 48 hours after the decision to intercept has been made, the authorisation given by the directorate officer should be for a period not exceeding 48 hours.

6.151 **We recommend that where the directorate officer reasonably believes that the criteria for the issue of a warrant are satisfied and the urgency of the situation necessitates the interception of communications before making an application to the court, he may, on such terms and conditions as he thinks fit, give authorisation to intercept a communication for a period not exceeding 48 hours.**

6.152 The authorisation given by the directorate officer should be granted in respect of communications originating from or received by persons whose communications are to be intercepted. It must never be framed as a blanket approval.

6.153 **We recommend that an officer who proposes to make an interception without prior authorisation of the court should apply for permission from a directorate officer on every occasion he proposes to do so. The permission to make an interception must be recorded in writing. Further, its terms and conditions must be specific.**

6.154 **We recommend that in applying for a warrant *ex post facto*, the officer should serve on the court :**

(a) an affidavit which includes particulars of the urgent situation because of which the applicant reasonably believed that it was impracticable for him to obtain prior authorisation from the court; and

(b) a copy of the authorisation given by a directorate officer authorising the interception of communications prior to making an application to the court.

6.155 **We recommend that -**

(a) where an interception is made without the prior authorisation of the court, the interception should terminate as soon as the purpose is achieved or when the application is denied by the court, whichever is the earlier; and

(b) where the *ex post facto* application is denied by the court, the interception should be treated as unauthorised and the material obtained as a result of the interception should be destroyed immediately.

6.156 The court may refer the matter to the Attorney General or the Court of Appeal whenever an application is denied.

6.157 Where the *ex post facto* application is not approved by the court, the directorate officer concerned may be at risk of criminal liability. We agree that the authorising officer or the officer making the interception should be liable if the court is satisfied that the officer had not been acting in good faith when authorising or making the interception.

6.158 **We recommend that where an *ex post facto* application is denied by a judge, the directorate officer authorising the interception of communications in an urgent situation, or the officer making an interception on authority of a directorate officer, should not be guilty of unlawful interception if the court is satisfied that the officer concerned acted in good faith when authorising or making the interception.**

6.159 There may be circumstances in which a warrant is issued but, through honest mistake, it does not adequately cover the interception which is subsequently carried out. The interception in such a case would be unlawful, even though a satisfactory warrant could have been applied for, and would have been issued, if the mistake had been realised at the outset. It would be unsatisfactory if the warrant were to be set aside and any intercepted materials destroyed.

6.160 **We therefore recommend that an application should be allowed to be made *ex post facto* to ratify an interception which was not covered by an existing warrant because of an honest error committed by the applicant, provided that -**

(a) the application is made within 48 hours of the applicant having notice of the error; and

(b) the interception would have been authorised if the applicant had applied for it at the time he made the original application.

The application should be accompanied by an affidavit which includes the particulars of the error committed by the applicant and how and when the error was discovered.

6.161 One respondent submitted that the number of judges who handle *ex post facto* applications should preferably be limited to three in order to provide greater consistency of decisions. Although it is desirable that the judges who are assigned to handle such applications should be limited in number so that the judges concerned can gain experience in the issuance of warrants, we believe this is a matter for the Judiciary to decide.

Right of appeal by the applicant

6.162 We do not consider it necessary to provide the person applying for a warrant with a right of appeal because it is always open to him to make a fresh application to the court. The risk of the applicant going on a fishing expedition is low because of our earlier recommendation that the applicant should swear an affidavit as to, *inter alia*, the number of instances on which an application has been made in relation to the same subject matter or target and whether that previous application was rejected or approved. In addition, we think that there would be practical difficulties of security associated with providing a right of appeal. In reality, we think it highly unlikely that the law enforcement agencies would choose to avail themselves of any right of appeal because of the risk that the security of the covert operation might be compromised.

Chapter 7

Material obtained from interception of communications

Summary

7.1 This chapter considers how intercepted material should be treated in order to meet privacy requirements. Topics covered include the following:

(a) safeguards relating to the retention of intercepted material;

(b) admissibility of material obtained through interception of communications carried out pursuant to a warrant;

(c) admissibility of material obtained through unlawful interception of communications; and

(d) the requirement to notify the target or "innocent" persons caught by the interception.

Recommendations and conclusions

7.2 On an application for a warrant authorising interception of telecommunications, the authorising judge shall make such arrangements as he considers necessary to ensure that -

(a) the extent to which the intercepted material is disclosed;
(b) the number of persons to whom any of the intercepted material is disclosed;
(c) the extent to which the intercepted material is copied; and
(d) the number of copies made of any of the intercepted material

is limited to the minimum that is necessary for the purpose for which the application was made. A transcript shall be treated as a copy of the intercepted material. This requirement will be satisfied if each copy made of any of the intercepted material is destroyed as soon as its retention is no longer necessary for the specified purpose.

7.3 Material obtained through an interception of telecommunications carried out pursuant to a warrant shall be inadmissible as evidence regardless of its relevance. For the purposes of this recommendation, "telecommunications" means communications by electromagnetic means. This prohibition should cover not only the fruit of interception but also the manner in which the interception was made.

7.4 No evidence shall be adduced and no question shall be asked in cross-examination which tends to suggest that an offence in relation to an interception of telecommunications has been committed or that a warrant authorising an interception of telecommunications has been issued.

7.5 There should be no discretion for the judge to admit material obtained through an interception of telecommunications carried out pursuant to a warrant.

7.6 Material obtained through an interception of communications transmitted other than by electromagnetic means which was carried out pursuant to a warrant shall be admissible as evidence and may be retained for so long as may reasonably be necessary for the purpose of any criminal proceedings.

7.7 Material obtained through an unlawful interception of telecommunications shall be inadmissible as evidence regardless of its relevance. This prohibition should cover not only the fruit of interception but also the manner in which the interception was made.

7.8 Material obtained through an unlawful interception of communications transmitted other than by electromagnetic means shall be admissible as evidence.

7.9 Material obtained through an interception of communications whether carried out with or without lawful authority shall be admissible in evidence in relation to proceedings for the offence prohibiting interception of communications.

7.10 Consideration should be given by law enforcement agencies to the destruction of material obtained by an unlawful interception of telecommunications, whether in whole or in part, as soon as the material is not reasonably necessary for the purpose of any investigation or criminal proceedings.

7.11 It is not necessary to require that the person whose communications have been intercepted be notified of that fact.

Safeguards regarding retention of material obtained by an interception of telecommunications carried out pursuant to a warrant

7.12 The sub-committee recommended in the consultation paper that provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985 should be adopted. Section 6 provides:

> *"(1) Where the Secretary of State issues a warrant he shall, unless such arrangements have already been made, make such arrangements as he considers necessary for the purpose of securing - (a) that the requirements of subsections (2) and (3) below are satisfied in relation to the intercepted material; ... .*
>
> *(2) The requirements of this subsection are satisfied in relation to any intercepted material if each of the following, namely -*
>
> *(a) the extent to which the material is disclosed;*
> *(b) the number of persons to whom any of the material is disclosed;*
> *(c) the extent to which the material is copied; and*
> *(d) the number of copies made of any of the material;*
>
> *is limited to the minimum that is necessary [for the purposes] mentioned in section 2(2) above.*
>
> *(3) The requirements of this subsection are satisfied in relation to any intercepted material if each copy made of any of that material is destroyed as soon as its retention is no longer necessary [for the purposes] mentioned in section 2(2) above."*

7.13 Under the United Kingdom scheme, the "shelf life" of intercepted material is strictly limited. Upon fulfilment of the specified purposes, the material obtained pursuant to the warrant must be destroyed and hence may not be used as evidence.

7.14 The United Kingdom model provides a practical approach. The destruction of the intercepted material protects the privacy of targets and innocent persons who had contacts with them. There would be no question of making full disclosure of the contents of communications to other parties to the proceedings. The problems arising from the disclosure of unused material could therefore be avoided. Imposing a requirement that intercepted material should be destroyed would also boost public confidence in the

warrant system. Furthermore, the secrecy of the manner in which the material was intercepted would not be compromised.[1]

7.15 The House of Lords in *Preston* agreed that privacy concerns and the need to maintain the secrecy of interception activities overrode the duty to make complete disclosure of unused materials:

> *"The need for surveillance and the need to keep it secret are undeniable. So also is the need to protect to the feasible maximum the privacy of those whose conversations are overheard without their consent. Hence sections 2 and 6. These policies are in flat contradiction to current opinions on the 'transparency' of the trial process. Something has to give way, and the history, structure and terms of the statute leave me in little doubt that this must be the duty to give complete disclosure of unused materials. The result is a vulnerable compromise, but it may be the best that can be achieved."*[2]

7.16 Destruction of intercepted materials does not mean that interception activities would not be subject to effective supervision. We discuss later measures for ensuring accountability.[3]

7.17 Two respondents, while agreeing to the destruction of primary material obtained through authorised interception, maintained that the investigator should be allowed to keep the intelligence gathered from such material.

7.18 It has never been our intention to prohibit the retention and use of analyses compiled on the basis of primary materials obtained through authorised interception (i.e. the secondary material or the so-called "fruits" of interceptions). Although the intercepted material (e.g. tapes and transcripts) would be destroyed under our proposals, the law enforcement agencies should be allowed to retain the analyses as intelligence in order to assist their investigations.[4] Any evidence collected in consequence of such investigations may be adduced in court by advising that the police were "acting on information received".

7.19 We note that there may be difficulties in prosecuting offenders if the communication discloses the existence of a conspiracy which is not carried into effect, but we believe that such cases are likely to be few and far between. In any event, other non-intrusive surveillance techniques would still be available to the law enforcement agencies. Indeed, if the interception was

---

1 *R v Preston* [1993] 4 All ER 638 at 677.

2 *Op cit*, at 669.

3 We shall recommend in the next chapter the creation of a supervisory authority to review the issue of warrants.

4 The use and storage of the analyses would, however, be subject to the provisions of the Personal Data (Privacy) Ordinance. For instance, an innocent person whose communications have been intercepted has the right to have access to his personal data held by the investigator unless one of the statutory exemptions applies (as when the materials are still required for the detection of crime).

performed with the consent of one of the parties to the communication, the intercepted material itself could be tendered in evidence because consensual interception would remain lawful under our proposals.

7.20 This approach apparently accords with current practice of the law enforcement agencies in Hong Kong. In 1992, the then acting Deputy Secretary of Security, Mr Clinton Leeks, advised the Legislative Council's Constitutional Development Panel that all interceptions were carried out in connection with investigations and were not used as a means of gathering evidence for court cases.[5]

7.21 Different considerations apply to intercepted material which is not obtained by an interception of telecommunications. Such material mainly consists of postal mail and documents printed from facsimile machines. The privacy concerns relating to these materials are not as great as those arising from an interception of telecommunications. The intercepted communication in the former case is specific to only two individuals, i.e. the sender and the intended recipient, and may have high evidential value in proving the guilt of a suspect. We therefore recommend below that this material should be admissible in evidence. With this in mind, it would be inappropriate to require the authorising judge to impose a requirement to destroy the intercepted material obtained by an interception of communications other than telecommunications. Our recommendation on the safeguards regarding retention of material obtained by an interception carried out pursuant to a warrant is therefore confined to material obtained by an interception of telecommunications.

7.22 **We recommend that on an application for a warrant authorising interception of telecommunications, the authorising judge shall make such arrangements as he considers necessary to ensure that -**

(a) the extent to which the intercepted material is disclosed;
(b) the number of persons to whom any of the intercepted material is disclosed;
(c) the extent to which the intercepted material is copied; and
(d) the number of copies made of any of the intercepted material

is limited to the minimum that is necessary for the purpose for which the application was made. A transcript shall be treated as a copy of the intercepted material. This requirement will be satisfied if each copy made of any of the intercepted material is destroyed as soon as its retention is no longer necessary for the specified purpose.

---

[5] *South China Morning Post,* 26 February 1992.

Admissibility of material obtained through interception of communications carried out pursuant to a warrant

7.23 The adoption of section 6 of the 1985 Act will have the result that evidence of the fruits of *authorised* interception of telecommunications can never be produced in court. The intercepted material and the copies thereof must be destroyed once its purpose (e.g. the prevention or detection of crime) has been served. However, a party might be in breach of the requirement to destroy the material and seek to adduce it in evidence. Further, the statutory requirements for destruction would not apply to material obtained by an authorised interception of communications other than telecommunications, or an interception which was not authorised by the court.

7.24 Under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence. The court has no power to exclude evidence merely because the judge disapproves of the way in which it was obtained, as, for example, where evidence was obtained unfairly or by trickery.[6] There is, however, a judicial discretion to exclude evidence if its prejudicial effect exceeds its probative value. The court also has inherent jurisdiction to make orders which are necessary to ensure a fair trial.

7.25 In determining whether to admit intercepted material in evidence, we need to take into account the probative value of the material and the privacy risk involved. High quality evidence collected by means which pose a low privacy risk should be admissible but low quality evidence collected by means which pose a high privacy risk should be inadmissible. Other factors include the purpose of the interception, the duration of the warrant, and the amount of relevant and irrelevant information obtained from the interception.

7.26 The sub-committee initially considered that intercepted material pertaining to the period preceding the laying of the charge should be admissible in the subsequent prosecution. Restricting the admissibility of evidence obtained as a result of an interception would have far-reaching results. It would mean that even if an interception reveals the sole evidence of a serious offence, that evidence may not be adduced. Similarly, evidence which assists an accused, such as an attempt to fabricate evidence against him, may not be adduced if it was obtained by interception, even though the interception was authorised by the court.

Material obtained through interception of telecommunications

7.27 While evidence arising from interception of telecommunications is not usually admitted in Hong Kong, in a recent major drug case it was.[7] We

---

6 *R v Cheung Ka-fai* [1995] HKLR 184 at 195. The test of admissibility of evidence in Hong Kong is governed by the common law as expressed in *R v Sang* [1980] AC 402 at 432-3.

7 *R v Cheung Ka-fai* [1995] HKLR 184. The calls in that case were intercepted by the Royal Canadian Mounted Police.

note that the laws of the United States,[8] Canada,[9] and Australia[10] regulating the interception of telecommunications all countenance the admission of lawfully intercepted material as evidence in prosecutions.

7.28 We recommended at the beginning of this chapter that material obtained by an interception of telecommunications should be destroyed as soon as its prescribed purpose has been fulfilled. Admitting in evidence material obtained through an interception of telecommunications would require its retention for this purpose. This would run counter to our recommendation on destruction of intercepted material. It also gives rise to the problem of disclosure of unused material to the defence. Generally, only a small part of the intercepted material would be used by the prosecution as evidence. But since the prosecution is under a duty to disclose all material information, all unused material would probably have to be made available to the defence.[11]

7.29 It is true that the court may impose appropriate conditions. For example, defence counsel may have to undertake not to divulge the contents of tapes played to them. But use of intercepted material as evidence will necessarily compound the invasion of privacy entailed in the original intrusion. There is always a risk of *public* dissemination of personal information contained in the intercepted communications. Furthermore, the present legal status of unused material is vexed and is subject to a number of appeals.

7.30 A further complication which is avoided by prohibiting the use of intercepted material as evidence arises from the application of public interest immunity.

7.31 In view of the risk of public dissemination of intercepted information and the difficulties with disclosure of unused material, the sub-committee recommended in the consultation paper that material obtained through an interception of communications should be inadmissible as evidence, regardless of its relevance.

7.32 Implementing the recommendation in the consultation paper necessitates the adoption of a provision similar to section 9 of the United Kingdom Interception of Communications Act 1985. This section prohibits any reference to authorised or unauthorised interception of telecommunications and mail. Subsections (1) and (2) state:

> *"(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest -*

---

8 Wiretap Act, sections 2515 and 2518(9) & (10)(a).

9 Criminal Code, section 189(5). Notice of intention to introduce evidence of lawfully intercepted communications must be given to the accused.

10 Telecommunications (Interception) Act 1979, section 74.

11 *R v Preston* [1993] 4 All ER 638 at 664. The test for whether unused material should be disclosed by the prosecution to the defence is materiality, not admissibility.

(a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below; or

(b) that a warrant has been or is to be issued to any of those persons.

(2) The persons referred to in subsection (1) above are -

(a) any person holding office under the Crown;

(b) the Post Office and any person engaged in the business of the Post Office; and

(c) any public telecommunications operator and any person engaged in the running of a public telecommunication system."

7.33 It appears that section 9(1) would not prevent the admission of evidence and cross-examination in the exceptional cases where there can be an interception without an offence being committed (e.g. because of consent) where no warrant is in existence.

7.34 The United Kingdom Government hoped that by making intercepted material generally inadmissible in legal proceedings, it would ensure that interception could be used only as an aspect of investigation, not of prosecution.[12] However, the Court of Appeal in *Effik* held that section 9 does not provide that evidence obtained as a result of an interception would be inadmissible:

> *"The forbidden territory is drawn in a much narrower fashion. And there is a logical reason for the narrow exclusionary provision. That is the reflection that it cannot be in the public interest to allow those involved in espionage or serious crime to discover at a public trial the basis on which their activities had come to the notice of the Police, the Customs and Excise or the Security Services, such as, for example, by questions designed to find out who provided the information which led to the issue of the warrant. So interpreted section 9(1) makes sense. And it would make no sense to stretch that language to become a comprehensive exclusion of all evidence obtained as a result of any interception."*[13]

7.35 The Court of Appeal in *Preston* agreed that section 9 does not operate to render inadmissible in evidence the contents of the intercepts. However, the effect of a literal application of the language of section 9(1) would, other than possibly in the most exceptional case, be to prevent any material derived from an interception being adduced in evidence. The court explained:

---

12 *Interception of Communications in the United Kingdom* (Cmnd 9438, 1985), clause 12(f).

13 *R v Effik* (1992) 95 Cr App R 427 at 432.

"In order to lay the groundwork for material to be admissible in evidence the manner in which the material has been obtained will normally have to be given in evidence in court and this will in turn tend to suggest either an offence under section 1 has been committed or a warrant has been issued which therefore contravenes section 9. It is this evidence of how the material was obtained which is the 'forbidden territory' and the fact that it should not be adduced in evidence will also usually prevent the material which was obtained as a result of the interception being given in evidence."[14]

7.36 The result is that it is normally not possible to adduce any evidence obtained as a result of an interception to which the 1985 Act applies. Such a prohibition would cover not only the fruits of interception but also the manner in which the interception was carried out. But if the parties were by agreement or admission to put the material before the court, it appears that there is nothing in section 9 to prevent this.[15]

7.37 In Hong Kong there is no bar to the defence raising the issue of interception, provided it is relevant to the case. In practice, it is extremely rare for material obtained through interception of telecommunications to be used as evidence in court. A provision in similar terms to section 9 would render any reference to interception activities inadmissible, whether or not it was authorised. As far as interception of telecommunications is concerned, this would mean that no evidence could be adduced and no question could be asked in cross-examination, which tended to suggest that an offence in relation to the interception of telecommunications had been committed or that a warrant authorising an interception of telecommunications had been issued.

7.38 One respondent to the consultation paper was concerned that the proposal on inadmissibility would preclude the suspect from confronting the basis of an investigation. The suspect might have contended that the intercepted communication had been misinterpreted by the law enforcement agency and, as a result of that mistake, the agency had triggered an elaborate investigation leading to his prosecution. We reiterate that the intercepted material would be used only for intelligence and not as a basis for the decision whether or not to prosecute. Although the suspect would not have an opportunity to correct any mistake made by the agency in compiling the analyses, he would still be able to confront in court the admissible evidence collected on the basis of the intercepted material should a prosecution ensue.

---

14 *R v Preston* (1992) 95 Cr App R 355 at 365.

15 The House of Lords explained that this point is of little or no importance in practice because if the regulatory system is working properly the material will have been destroyed long before the trial, and if it is favourable to the accused the prosecution will not have been pursued: *R v Preston* [1993]4 All ER 638 at 672. As section 6 of the 1985 Act requires the destruction of intercepted material once a charge is laid against the accused, the purpose of section 9 can be seen as the protection, not of the fruits of the interception, but of the information as to the manner in which they were authorised and carried out: *op cit,* at 667.

7.39 The Bar Association found it unsatisfactory that lawfully obtained material which may be the only evidence of a crime cannot be used at trial, but instead has to be destroyed. They preferred a regime which would allow the prosecution to decide whether, and to what extent, material obtained pursuant to a warrant is retained and used.

7.40 Other respondents also had reservations on our proposals. The Hong Kong Alliance of Chinese and Expatriates held the view that judges should see as much evidence as was available, particularly when it would be the court which would authorise any intrusion. The Alliance wanted to see a regime in which the prosecution must reveal that intrusive measures had been applied. The Liberal Democratic Federation of Hong Kong was concerned that the work of the law enforcement agencies would be hindered and the deterrent effect weakened if material obtained by interception was inadmissible. They therefore proposed to give the court a discretion to admit such material as evidence depending on its usefulness.

7.41 There were, however, others who agreed with the proposal that intercepted material should be inadmissible. One respondent commented that the legislation should expressly provide that intercepted material should be exempted from pre-trial disclosure to the defence. We agree with this comment in principle. We understand that the law enforcement agencies are satisfied that the adoption of the proposal regarding inadmissibility of intercepted material would not undermine their efforts in fighting crime. Indeed, making intercepted material inadmissible would protect the safety of those who are engaged in covert activities because details of the conduct of an interception would not be made public.

7.42 Material gleaned from an interception is often not specific. Since interception of telecommunications normally lasts for weeks or even months, it is highly likely that personal information which is not relevant to the investigation would be acquired. Much of the information obtained by investigators would probably relate to "innocent" parties who have had contacts with those targeted for interception. If the intercepted material were admissible, this would inevitably result in an invasion of the privacy both of innocent parties and of the target himself. From a privacy point of view, the person whose privacy has been affected by an interception ought to be notified that his right to privacy has been infringed. Problems relating to notification then arise. Who should be notified of an interception? Of what should he be notified? Under what circumstances should he be notified? And when should he be notified? All these problems could be avoided if the privacy of the person affected by an interception could be safeguarded by the destruction of the intercepted material and the rendering of that material inadmissible in court.

7.43 The preceding discussion explains that the principal purpose of interception of telecommunications is the *gathering of intelligence*, and not the collection of evidence for use in prosecutions. It will be recalled that one of the grounds for the issue of warrants is the "prevention or detection" of serious crime, not the "prosecution" of serious crime. As interception of

telecommunications (including telephone tapping) poses a high privacy risk but normally generates material of low probative value, we maintain that material obtained through an interception of telecommunications should be inadmissible in evidence.

7.44 **We recommend that material obtained through an interception of telecommunications carried out pursuant to a warrant shall be inadmissible as evidence regardless of its relevance. For the purposes of this recommendation, "telecommunications" means communications by electromagnetic means. This prohibition should cover not only the fruits of interception but also the manner in which the interception was made.**

7.45 **We recommend that no evidence shall be adduced and no question shall be asked in cross-examination which tends to suggest that an offence in relation to an interception of telecommunications has been committed or that a warrant authorising an interception of telecommunications has been issued.**

Material obtained through interception of communications transmitted other than by electromagnetic means

7.46 Different considerations apply, however, to material obtained through an interception of postal mail. An intercepted letter may contain an instruction to kill someone, or a confession by a murderer that he has killed a person. Dangerous drugs may also be discovered in the postal packet. These materials may be crucial evidence to the prosecution. Furthermore, postal mail is a discrete form of communication between only two individuals who can easily be identified. The privacy risk of admitting such materials is therefore low but the probative value of the intercepted material might be great. The privacy concerns associated with the disclosure of unused material are also less than would be the case with intercepted telecommunications because intercepted material would be specific and the information obtained would invariably relate to the suspect. In contrast to material obtained by an interception of telecommunications, admission of intercepted mail in evidence is not infrequent even though both types of material are admissible under existing law. We therefore conclude that material obtained through interception of postal mail should continue to be admissible in evidence and may be retained for so long as may reasonably be necessary for the purpose of any criminal proceedings. Where the intercepted material is not required, or is no longer required, for any criminal proceedings, it should be returned to the addressee provided that this would not prejudice any current or future investigations.[16]

7.47 Similar considerations should also apply to the interception of that part of a communication which consists of a physical document. What we have in mind are those communications which are transmitted by two

[16] Cf Post Office Ordinance (Cap 98), section 14.

different means of communication before they reach the hands of the intended recipient. For example, a facsimile transmission to the addressee would first be transmitted by electromagnetic means in the form of electronic signals to a facsimile machine at the receiving end. On receipt of the message, the facsimile machine converts the electronic signals into a physical document. The document is then transmitted by hand to the intended recipient. While communications on a telecommunication line may involve different sorts of data relating to many individuals, a document resulting from the facsimile transmission would be privy only to two individuals. As the privacy concerns and evidential value of facsimile copies or other documents transmitted in similar circumstances are of the same magnitude as those of physical objects delivered by postal mail, material obtained through an interception of communications transmitted other than by telecommunication should be admissible.

7.48 In conclusion, although material obtained through an interception of telecommunications (meaning communications transmitted by electromagnetic means) should not be admissible in evidence, material obtained through an interception of communications transmitted other than by electromagnetic means should continue to be admissible as under existing law.

7.49 **We recommend that material obtained through an interception of communications transmitted other than by electromagnetic means which was carried out pursuant to a warrant shall be admissible as evidence and may be retained for so long as may reasonably be necessary for the purpose of any criminal proceedings.**

Discretion to admit material obtained through an interception of telecommunications carried out pursuant to a warrant

7.50 There may be rare instances where the only evidence available is a statement made in a telephone conversation. For example, a suspect may telephone a contract killer asking him to kill someone. Neither the fact of the tap nor the transcript of the intercepted conversation would be admissible under our proposals. Putting aside the question whether the parties to the communication can be identified, should the prosecution be allowed to apply to the court for permission to use the intercepted material as evidence under a strictly controlled exception?

7.51 It has also been suggested that evidence obtained from a duly authorised interception (excluding that obtained by virtue of an *ex post facto* warrant) should be admissible, with the judge having a discretion to exclude the evidence if its prejudicial effect outweighs its probative value. Such an approach would provide judicial control at both ends of the process: first when the original application for a warrant was made, and later when the judge considered the value of the evidence.

7.52 We have considered the arguments for and against creating an exception to the inadmissibility of intercepted material. We believe considerable problems would arise if the fruits of telephone tapping were to be rendered admissible in exceptional circumstances. How much of the intercepted material may, or should, be retained by the law enforcement agencies? Would the provision of such an exception be open to abuse by the prosecution or defence?

7.53 In principle, all intercepted materials pertaining to the case should be retained if any part of the conversation would be used as evidence in subsequent prosecution. If the agencies were allowed to apply for permission to adduce in evidence material obtained through an interception of telecommunications, *all* materials intercepted pursuant to a warrant would have to be kept at least until completion of an investigation (which may last for a considerable time) so as to enable the agencies to decide whether the material is required for use as evidence. The importance of a piece of evidence could never be known until the entire investigation had been completed; and if the agencies were allowed to keep the material for such purposes, all attempts to protect privacy through the destruction of intercepted material would be put at naught. Retention of intercepted material would also give rise to the problems arising from disclosure of unused material noted above.

7.54 The reality of the situation is that the law enforcement agencies are unlikely to make use of such an exception even if it is provided. In order to introduce in evidence the intercepted material, the prosecution would have to show a proper chain of evidence. That would inevitably reveal the fact of an interception and the details of the covert operation. If the *modus operandi* of such an operation were made public, the safety of the persons engaged in such activities would be put at risk and the efficiency of the agencies would be undermined.

7.55 While intercepted material may be extremely useful in terms of intelligence, it is unlikely to be of much value in proving criminal intent. It is extremely rare that vital evidence can be obtained through interceptions. Statements made in a telephone conversation are always open to different interpretations and it is improbable that a criminal would make his intention clear when communicating over the phone. The chances are remote, for instance, that the contract killer would be subject to an interception at the precise moment when he voiced his avowed intent to carry out his next homicide.

7.56 We believe that exceptional situations such as those referred to are extremely rare. Even if the legislation does not provide for an exception, criminal intelligence gathered from intercepted material would often lead to other evidence that is admissible in court. Further, the law enforcement agencies still have two weapons in their hands. They may either conduct surveillance on one or other of the parties to the communication, or collect evidence with the assistance of an informer or undercover officer by relying

on the exception of one-party consent. Material obtained by such means will continue to be admissible in evidence.

7.57 Despite the superficial attractions of providing for an exception, the practical problems accompanying this concept appear to be overwhelming. We therefore conclude that there should be no discretion for the judge to admit material obtained through an interception of telecommunications carried out pursuant to a warrant. It follows that no reference can ever be made to an interception of telecommunications, or to the possibility of such an interception, in any proceedings, either in examination-in-chief or cross-examination.

Admissibility of material obtained through unlawful interception of communications

7.58 The United States law prohibits the admission of illegally obtained evidence. The contents of any wire or oral communications intercepted pursuant to the Wiretap Act (or evidence derived therefrom) may not be received in evidence if the communication was unlawfully intercepted or the interception was not made in conformity with the order of authorisation.[17]

7.59 Supporters of this approach argue that this both discourages illegal methods and concentrates the minds of investigators on more straightforward means of investigation. But deeming illegally obtained surveillance material inadmissible would not preclude investigators from using it during the investigation, such as confronting suspects with the material to elicit confessions.

7.60 We have recommended that material obtained through authorised interceptions of telecommunications shall be inadmissible. It would be an anomaly if we now recommend that material obtained through *unauthorised* interceptions would be admissible. Such a recommendation can only encourage intruders to resort to unlawful interceptions which do not have the scrutiny of the court. In our opinion, material obtained through interception carried out without court authorisation should be admissible only if one of the parties to the communication has consented to the interception.

7.61 **We recommend that material obtained through an unlawful interception of telecommunications shall be inadmissible as evidence regardless of its relevance. This prohibition should cover not only the fruits of interception but also the manner in which the interception was made.**

7.62 For the same reasons given in paragraphs 7.46 and 7.47 above, material obtained through *unlawful* interception of communications transmitted other than by electromagnetic means should be admissible.

[17] Wiretap Act, section 2515 and section 2518(9) and (10)(a).

Admitting such materials, however, would not affect the criminal liability of persons who intercepted the communications without authority.

7.63 **We recommend that material obtained through an unlawful interception of communications transmitted other than by electromagnetic means shall be admissible as evidence.**

Admissibility of intercepted material in relation to proceedings for unlawful interception of communications

7.64 We agree that there should be an exception to allow evidence of interceptions to be adduced in court to prosecute an individual who is alleged to have committed the interception offence.

7.65 **We recommend that material obtained through an interception of communications whether carried out with or without lawful authority shall be admissible in evidence in relation to proceedings for the offence prohibiting interception of communications.**

Safeguards regarding retention of material obtained by unlawful interception

7.66 Although all material obtained by an interception of telecommunications carried out pursuant to a warrant would have to be destroyed in compliance with the conditions imposed by the judge, material obtained through *unlawful* interception would not be subject to this statutory requirement. In investigating a criminal case, the police might discover material which was obtained as a result of an unlawful interception. Although this material may be used as evidence of unlawful interception if the offender could be brought to trial, there is no guarantee that it would be destroyed if the investigation resulted in no prosecution and the case is closed. Even if a prosecution is brought against the offender, the material might be retained for years so as to ensure that evidence is still there in case leave is granted for the accused to appeal out of time.

7.67 In order to meet privacy requirements, **we recommend that consideration should be given by law enforcement agencies to the destruction of material obtained by an unlawful interception of telecommunications, whether in whole or in part, as soon as the material is not reasonably necessary for the purpose of any investigation or criminal proceedings.**

Discretion to exclude evidence unlawfully obtained

7.68 The Hon James To referred us to sections 76 and 78 of the United Kingdom Police and Criminal Evidence Act 1984. He suggested that

in considering whether the intercepted material is admissible, the court should examine -

(a) whether the material was obtained lawfully;
(b) whether the granting of the warrant was legal, reasonable and proper; and
(c) whether the admission of such evidence would have an adverse effect on the proceedings.

7.69 Mr To is in effect suggesting that the court should have a power to exclude unfairly obtained evidence. This is a departure from existing law because generally speaking a judge has no discretion to exclude relevant admissible evidence merely because it had been improperly obtained. As the suggestion covers all types of evidence, whether or not they were obtained by interception of communications, it is a matter beyond our current remit.

Notification following termination of interception

The notification requirement

7.70 A requirement that the object of interception be notified of the fact that he had been subject to interception once it is terminated is a feature of some but not all laws. In the United States, the Wiretap Act requires that "the persons named in the order or application, and such other parties to intercepted communications as the judge may determine" be notified of the period of interception and such portions of the intercepted communications as the judge may determine.[18] The Canadian Criminal Code also provides that the person who was the object of an authorised interception be notified of that fact. The notice, however, need not include the contents or details of the authorisation.[19] In Germany, "[m]easures of restriction shall be notified to the person concerned after they are discontinued".[20]

7.71 Merely to inform an individual of the fact that he has been the object of interception would serve little purpose. More helpful and informative would be to notify the former target of the sorts of matters covered by the United States provision, including, where appropriate, providing portions of the intercepted communications themselves. We understand that under current Hong Kong practice often only key points from the intercepted communications will be abstracted and retained.

---

18 Section 2518(8)(d).

19 Section 196.

20 German Act on Restriction of Privacy of Mail, Posts and Telecommunications 1989, section 5(5). Indeed one aspect of the German law which was challenged in *Klass* is that there was no requirement that the object of interception be *invariably* notified upon its cessation. The European Court held that this was not inherently incompatible with the privacy provision of the European Convention, provided that the person affected be informed as soon as this could be done without jeopardising the purposes of the interception.

The basis of notification requirement

7.72 The basis of a notification requirement is two-fold. First, it marks the seriousness of the earlier intrusion into privacy. The requirement would introduce an important element of accountability and should deter the authorities from intercepting unnecessarily.

7.73 Secondly, the individual should be able to challenge the grounds on which the intrusion was allowed. Denying the target information that he has been the object of interception will limit the efficacy of the mechanisms enhancing accountability, such as review procedures and the provision of compensation awarded for wrongdoing. We note that the United Kingdom Act lacks a notification requirement and, although compensation is provided for, no claim to date has been successful.

7.74 We think that the public has a right to be told the extent to which intrusions are occurring, although this would partly be addressed by the public reporting requirements to be recommended by us in the next chapter. The adoption of a notification requirement would diminish the need for mechanisms at the stage when the warrant is approved, such as the participation of a third party in the *ex parte* proceedings to represent the interests of the target.[21] There are, however, practical problems in implementing this requirement.

Practical problems of notification

(a) The conflict between notification and the purposes of interception

7.75 A notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of law enforcement agencies would not be diminished. The requirement would have to be couched in terms that, following the termination of interception, the targets and, perhaps, those innocent parties affected by the interception, should be notified unless this would "prejudice" the purposes of the original intrusion. There would also need to be provision for postponement of the notification on the same grounds.

7.76 "Prejudice", in relation to the target, could be defined to cover the situation where the target is likely to be the object of surveillance or interception in the future and notification is likely to make such surveillance or interception more difficult. This approach would preclude notification of recidivist offenders, or those where there is a reasonable prospect that the investigation may be reopened in the future.

7.77 In the case of notification of "innocent" persons, the most obvious ground on which notification would be denied is if they could be expected to alert the target. Another possibility is that the authorities may

[21] E.g. the participation of a "friend of the court".

wish to tap the innocent person in order to further tap the target again and alerting the innocent person may make this more difficult.

7.78 The United Kingdom approach is that interception is necessarily clandestine and merely divulging that it has occurred would diminish the value of interception.[22] This obviously runs counter to any requirement of notification.

(b) Prolonged retention of intercepted material

7.79 If part of a notification requirement is to be that details of the fruits of an interception are to be disclosed following the termination of the interception, this necessarily implies that those materials must be retained. This has its own privacy risks.

(c) Resource implications

7.80 If the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected, applying criteria along the lines described above. Consideration would need to be given to the extent of information to be given to the target under a notification requirement. This raises potentially complex issues and would require the relevant authority to be well briefed on a case by case basis, applying the prejudice test outlined above. The resource implications are obvious. We recommend below that decisions impinging on interceptions should be capable of review. If decisions regarding notification are similarly to be reviewed, the resource implications will be even greater.

The need for notification

7.81 We have recommended that material obtained through interception of telecommunications shall be destroyed immediately after the interceptions have fulfilled the purpose. Destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism.[23]

7.82 We have also recommended that material obtained through an interception of telecommunications shall be inadmissible in evidence. If intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the risk to privacy, could be reduced to the minimum. There is therefore less need for a notification requirement in Hong Kong than in other jurisdictions where intercepted material may be produced at the trial.

---

22 *R v Preston* [1993] 4 All ER 638 at 648. It is a case on the interception of telephone communications.

23 We recognise that "destruction" is not an absolute concept in the digital age.

7.83 We note that the practice in the United States and Canada is only to notify the public of the fact of interception. It is presumably due to this that those jurisdictions do not appear to have encountered the difficulties we envisage may result from a more extensive notification requirement. We think that a restricted notification requirement along the lines of that in the United States and Canada is of little benefit. Finally, we believe that the accountability aspect is more directly addressed by the warrant system and the public reporting requirement. We have therefore concluded that a person whose telecommunications have been intercepted need not be notified of the interception.

7.84 As regards material obtained by an interception of communications transmitted other than by telecommunication (for example, letters and facsimile copies), although they will not be subject to a destruction requirement and will continue to be admissible in court, we do not think that any privacy problems arise. If the material was adduced in evidence, the suspect would have a right to challenge it in court; and if the material was not required or no longer required for any criminal proceedings, it should have been returned to the addressee or the sender, as the case may be, unless this would prejudice current or future investigation. Further, where one of the parties to the communication is aggrieved by the interception, he may ask for a review under the procedures recommended in Chapter 8 below. It is therefore not necessary for the persons communicating other than by telecommunication to be notified of the fact that his communications had been intercepted or interfered with.

7.85 In conclusion, it is not necessary to provide for a requirement that the object of an interception of communications be notified of the fact that he had been subject to interception. In coming to this conclusion, our main concerns are that such a scheme would have considerable resource and privacy implications, without a clear concomitant benefit. The only exception to this conclusion is where a warrant has been set aside by a judge or the supervisory authority concludes that a warrant had been improperly issued or complied with. We shall explain this in detail in Chapter 8 below.

Conclusion

7.86 Interception of communications enables the authorities to obtain information relating to individuals. As shown in this chapter, there are basically two routes to protecting privacy interests in intercepted material :

(a) Allow lawful intercepts to be admissible in evidence but the target would be notified of the fact that he had been subject to interception so that he may ask for a review if he is aggrieved by the interception. This approach necessitates the retention of material obtained by lawful interception, even though the purpose for which the interception was authorised had been fulfilled.

(b) Destroy the intercepted material and exclude it from evidence. However, the target would not have a right to be notified of the interception.

7.87 While Canada and the United States opt for the first approach, we have decided to follow the United Kingdom model in (b) in the case of interception of telecommunications. Notification is neither practical nor effective in protecting the individual against the privacy risk which would flow from admitting in evidence material obtained from an interception of telecommunications. Although the target would be deprived of a right to be notified, his privacy would receive greater protection than that under the first approach if all intercepted materials were destroyed and inadmissible in court. We believe this approach would not pose any problem to the law enforcement agencies because the primary purpose of the interception has always been to gather intelligence to assist their investigation. Indeed the agencies would be most reluctant to disclose in court the manner in which intercepted material has been obtained. Moreover, if material obtained from lawful interceptions were admissible, it could be argued that material from unlawful interceptions should also be admissible.

7.88 By imposing a requirement to destroy all material obtained by an interception of telecommunications carried out pursuant to a warrant, and rendering inadmissible in evidence material obtained through both lawful and unlawful interceptions of telecommunications, the privacy of the individual would be effectively protected without compromising the secrecy of interception activities or undermining the ability of the law enforcement agencies to fight crime.

Chapter 8

Compliance enforcement: supervisory authority and remedies

Summary

8.1 We examine in this chapter alternative approaches to the supervision of the warrant system and explore what remedies should be available to an aggrieved person whose communications have been unlawfully intercepted. In coming to our conclusions, we have examined the position in the United Kingdom, the United States and Australia.

Recommendations

8.2 (a) A supervisory authority should be created to keep the warrant system under review.

(b) A sitting or former judge of the Court of Appeal should be appointed by the Governor, on the recommendation of the Chief Justice, as the supervisory authority.

(c) The person appointed as the supervisory authority should hold office for a period of three years and should be eligible for reappointment for a further period of three years.

8.3 (a) The supervisory authority should have power to examine on his own initiative whether a warrant has been properly issued and whether the terms of a warrant have been properly complied with.

(b) The supervisory authority may -

(i) summon before him any person who is able to give any information relating to his review and examine that person for the purposes of such review;

(ii) administer an oath for the purposes of the examination under (i) above; and

(iii) require any person to furnish to him any information (on oath if necessary) and to produce any document or thing which relates to his review.

(c) The supervisory authority shall apply the principles applied by a court on an application for judicial review in reviewing the issue of warrants.

8.4 (a) An aggrieved person who believes that his communications have been unlawfully intercepted may request the supervisory authority to investigate whether there has been a contravention of the statutory requirements relating to the issue of warrants.

(b) Where the supervisory authority ascertains that there is a warrant affecting the aggrieved person which is still effective, he shall refer the case to the High Court.

(c) On referral of the case from the supervisory authority, a judge of the High Court (preferably the one who originally issued the warrant) shall review the case and decide whether the warrant has been properly issued and complied with.

(d) The review shall be conducted ex parte and the judge may examine any person and require him to furnish any information, document or thing that is relevant to the case.

(e) Where the reviewing judge is satisfied that the warrant has been properly issued and complied with, he shall affirm the warrant and notify the supervisory authority accordingly.

(f) Where the judge concludes that the warrant has been improperly issued or complied with, he shall -

(i) set the warrant aside; and

(ii) unless the intercepted material may be required for the purposes of establishing the illegality of the interception, order the destruction of the intercepted material.

(g) After setting the warrant aside, the judge shall refer the case back to the supervisory authority.

(h) The decision of the judge who reviews the case on referral by the supervisory authority shall be final.

(i) Where the warrant affecting the aggrieved person has expired, the supervisory authority shall review whether the warrant had been properly issued and complied with and will have the same power as a judge in dealing with the intercepted material.

(j) Any decision of the supervisory authority shall be final.

8.5 (a) Where the reviewing judge has set aside a warrant or the supervisory authority concludes that the warrant had not been properly issued or complied with, the supervisory authority shall notify the aggrieved person that there has been a contravention of the statutory requirements relating to the issue of warrants.

(b) In any other case, the supervisory authority shall refrain from making any comments other than informing the aggrieved person that there has been no contravention of the statutory requirements relating to the issue of warrants.

(c) The supervisory authority should have power to delay notification if he is satisfied that this would seriously hinder existing or future investigation of serious crime or prejudice the security of Hong Kong.

8.6 (a) The supervisory authority should have power to pay compensation to the aggrieved person out of public funds if the authority concludes that the warrant has been improperly issued or complied with, or if the warrant has been set aside by the reviewing judge.

(b) The aggrieved person should not be allowed to claim damages in court if he has already been awarded compensation by the supervisory authority.

8.7 Where there is evidence suggesting that a crime has been committed by the applicant in obtaining the warrant or by the person executing the same, the supervisory authority may refer the matter to the Attorney General to consider whether to bring criminal proceedings against the offender.

8.8 The supervisory authority should furnish annually a public report to the Legislative Council.

8.9 There should be a statutory requirement that the following matters be covered by the report to be furnished by the supervisory authority:

(a) the number of warrants applied for, withdrawn, rejected, granted as requested and granted subject to modifications;

(b) the average length of warrants and their extensions;

(c) the classes of location of the place at which communications were to be intercepted, e.g. domestic, business etc.;

(d) the types of interception involved, e.g. interception of telecommunications, interception of mail etc.;

(e) the major categories of serious crime involved;

(f) statistics relating to the effectiveness of interception in leading to the arrest and prosecution of those charged with serious crime;

(g) the number of reviews conducted by the supervisory authority in response to a request by an aggrieved person and an overview of such reviews; and

(h) the findings and conclusions of the review conducted by the supervisory authority in respect of the application of the warrant system.

8.10 The supervisory authority should furnish annually a confidential report to the Governor. The report should cover such matters as are required by the Governor, or considered relevant by the supervisory authority.

8.11 All licensed telecommunications carriers should be required to furnish quarterly reports to the Telecommunications Authority for onward transmission to the supervisory authority. The quarterly reports should provide information relating to the following matters:

(a) acts done by employees of the licensed carriers to assist the interception of telecommunications under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the average length of time during which telecommunications were intercepted under warrants which have expired within the reporting period.

8.12 The Post Office, the Customs and Excise Service and the courier companies should furnish quarterly reports to the supervisory authority containing the following matters:

(a) acts done by their employees to assist the interception of postal mail under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the total number of items intercepted.

8.13 Any person who intercepts a communication unlawfully should be liable to pay compensation to the person who suffers damage by reason of the unlawful interception unless the latter has been awarded compensation by the supervisory authority. Damage should be defined as including injury to feelings.

8.14 The remedy to be granted by a court in a civil action for unlawful interception may include an order requiring the defendant to pay punitive damages to the aggrieved party.

OVERSEAS JURISDICTIONS

The United Kingdom

8.15 The Interception of Communications Act 1985 establishes two distinct authorities, namely a supervisory authority and a complaints Tribunal.

Supervisory body

8.16 Section 8 of the 1985 Act establishes the post of Commissioner of Interception of Communications to "keep under review" the issue of warrants and the adequacy of arrangements to safeguard material obtained from interceptions. The appointee shall be "a person who holds or has held high judicial office". In practice, the appointee has been a sitting judge.

8.17 In his annual reports to the Prime Minister, the Commissioner refers to his "visits" to agencies "to investigate a range of warrants selected across the board, and to question those responsible for carrying out the interception."[1] Lustgarten and Leigh elaborate:

> *"In practice, the Commissioner devotes two periods a year away from judicial duties to the office. Review follows randomly selected warrant applications by reading individual files and talking to the officers involved. For this purpose he maintains a base in the Home Office, because of ease of access to the papers and personnel involved. The Commissioner also visits establishments (including intelligence and security establishments) and the ministers responsible for issuing warrants. This process involves looking not merely at the minister's decision but also at the accuracy and completeness of the information submitted with the warrant application."*[2]

8.18 In determining whether a warrant should have been issued, the Commissioner applies the test "could a reasonable Secretary of State form the view that a warrant is necessary?". This is the same test as is applied in judicial review. To date, no warrant has been found to fail that test.[3]

---

1 *Report of the Commissioner for 1994* (London, Cm 2828, 1995), paragraph 4.
2 Lustgarten and Leigh, *op cit,* at 63.
3 *Ibid,* at 62.

8.19 In addition to this selection of a sample of warrants for close examination, the Commissioner also refers in his annual report to the standard practice whereby the department would draw his attention to any case in which a procedural error or contravention of the 1985 Act has occurred.[4] Accordingly, the Commissioner refers in the last three annual reports to errors brought to his attention. This reliance on self-reporting leads Lustgarten and Leigh to come to the following conclusion:

> *" Although the office of Commissioner is a useful check, in practice it is probably the knowledge in Whitehall that the office exists, rather than the weak standard of review applied, which exerts most influence to ensure that the Act is followed carefully. A judge seconded part-time for a few days or weeks each year is not in a position to subject the entire process to in-depth scrutiny. "*[5]

Remedies

8.20 Section 7 of the Interception of Communications Act 1985 provides a quasi-judicial remedy by establishing a complaints tribunal which comprises lawyers of not less than 10 years' standing. Any person who believes that his communications have been intercepted may apply to the Tribunal for an investigation. Whereas the Commissioner's review duties are ongoing, the Tribunal's review role is based on complaints.

8.21 Where the Tribunal, applying the principles applicable on an application for judicial review, concludes that there has been a contravention of the statutory requirements in relation to a warrant issued under the Act, it shall give notice to the applicant stating that conclusion (but not the reasons) and report its findings to the Prime Minister. It may also make an order to do one or more of the following:

(a) quash the warrant;
(b) direct the destruction of copies of the intercepted material;
(c) direct the Secretary of State to compensate the applicant.

8.22 The decisions of the Tribunal are not subject to appeal or liable to be questioned in any court.

8.23 It is clear that the Tribunal may only investigate any breach of the requirements of the Act where a warrant has been issued. The Tribunal lacks jurisdiction if the alleged interception was not authorised by a warrant. It therefore provides no protection against unauthorised interceptions. Interceptions not sanctioned by any warrant are a criminal matter for investigation by the police. There is, however, no legal requirement that unauthorised interceptions be referred to the police.

---

4 *Report of the Commissioner for 1992,* (London, Cm 2173, 1993), paragraph 7.
5 *Op cit,* at 63.

8.24 The jurisdiction of the Tribunal is therefore limited to ascertaining whether a "relevant" warrant has been issued and, if so, whether it was issued on proper grounds and in the appropriate form. Since warrants are in practice only issued following careful vetting, Leigh comments that the Tribunal has been established "to deal with a problem that has never in fact arisen".[6] This is borne out by the fact that of the 250 cases considered in the first 6 years of operation of the Act, the Tribunal has not found a single breach. We examine below whether any supervisory role should extend not only to the investigation of authorised interceptions, but also to unauthorised interceptions.

Reports

8.25 The 1985 Act states that the Commissioner shall make an annual report to the Prime Minister "with respect to the carrying out of his functions".[7] A copy of the annual report has to be laid before each House of Parliament after the Prime Minister has excluded from the report any matter the publication of which would be prejudicial to national security, to the prevention or detection of serious crime or to the economic well-being of the United Kingdom.[8]

The United States

Reports

8.26 The Wiretap Act requires reports to be made at 3 levels:

(a) Within 30 days of the expiration of an order authorising interception (or each extension thereof) or the denial of an order, the issuing or denying judge has to report to the Administrative Office of the United States Courts:[9]

(i) the kind of order applied for;
(ii) the fact that the order was granted as applied for, was modified, or was denied;
(iii) the period of interceptions authorised by the order, and the number and duration of any extensions of the order;
(iv) the offence specified in the order or application;
(v) the identity of the applying officer; and
(vi) the nature of the facilities from which or the place where communications were to be intercepted.

---

6 I Leigh, "*A Tappers' Charter?*" (1986) *Public Law* 8, at 15.
7 Section 8(6). See also section 8(5).
8 Section 8(7) & (8).
9 Section 2519(1).

(b) The prosecuting authority has to make an annual report to the same Administrative Office on the following matters:[10]

(i) the information required in (a) above with respect to each application for an order made during the preceding year;
(ii) a general description of the interceptions made under such order;[11]
(iii) the number of arrests resulting from such interceptions, and the offences for which arrests were made;
(iv) the number of trials resulting from such interceptions;
(v) the number of convictions resulting from such interceptions, and the offences for which the convictions were obtained.

(c) The Director of the Administrative Office has to transmit to the Congress an annual report concerning the number of applications and the number of orders granted or denied during the preceding year. The report shall include a summary and analysis of the data in (a) and (b) above.[12]

Remedies

8.27 As with its data protection regime, the United States legislation on interceptions provides no administrative mechanism to deal with complaints about breaches of the statutory provisions. It is up to the individual to litigate.

8.28 A person whose communication has been intercepted in contravention of the Wiretap Act may claim damages in a civil action.[13] Such damages may include actual damages suffered by the plaintiff, profits made by the accused as a result of the contravention, and punitive damages in appropriate cases. It is a defence that there was a "good faith reliance" on a court warrant or order. Injunctive relief is also available to prevent a violation of the Wiretap Act.[14]

Australia

8.29 The Telecommunications (Interception) Act 1979 sets up a reporting system and provides for the granting of civil remedies to an aggrieved party. It also invests the Commonwealth Ombudsman with

---

10 Section 2519(2).

11 Including (a) the approximate nature and frequency of incriminating communications intercepted, (b) the approximate nature and frequency of other communications intercepted, (c) the approximate number of persons whose communications were intercepted, and (d) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions.

12 Section 2519(3).

13 Section 2520.

14 Section 2521.

additional functions and powers in relation to the interception of telecommunications.

Reports

(A) Reports to the Minister

8.30 Under the Telecommunications (Interception) Act 1979, reports have to be given to the Minister by the Commissioner of Police, the chief officer of a Commonwealth agency, and a telecommunication carrier.

(a) The Commissioner of Police is required to keep a Register of Warrants which contains the following particulars in relation to each warrant:[15]

(i) the agency to which the warrant was issued;
(ii) the telecommunications service to which the warrant relates;
(iii) the name of the person specified in the warrant as a person using or likely to use the telecommunications service;
(iv) the duration of the warrant; and
(v) the serious offence involved.

This register must be delivered to the Minister for inspection every three months.[16]

In addition, the Commissioner of Police must give to the Minister, within three months after a warrant has expired, a report about the acts done by the Federal Police in connection with intercepting communications under the warrant.[17]

(b) The chief officer of a Commonwealth agency is required to give to the Minister, within three months after a warrant has expired, a report containing:

(i) information about:
(1) the use made by the agency of information obtained by interceptions under the warrant,
(2) the communication of such information to persons other than officers of the agency; and
(3) the number of arrests that have been made on the basis of such information; and

(ii) an assessment of the usefulness of information obtained by the interceptions[18]

---

15 Telecommunications (Interception) Act 1979 (as amended), section 81A.
16 *Ibid*, section 81B. The Commissioner of Police must also deliver a Special Register of Warrants to the Minister under section 81D.
17 *Ibid*, section 98.
18 *Ibid*, section 94.

(c) A telecommunication carrier is required to give to the Minister within three months after a warrant has expired, a report about the acts done by its employees to enable communications to be intercepted under the warrant, and the days on which, and the times at which, those acts were done.[19]

(B) Reports by the Minister

8.31 The Minister must lay before each House of Parliament an annual report setting out the following particulars:[20]

(a) the relevant statistics about applications for warrant;
(b) the number of warrants issued;
(c) the categories of the serious offences specified in the warrants;
(d) the average duration of warrants;
(e) how many arrests were made on the basis of lawfully obtained information;
(f) the number of prosecutions in which lawfully obtained information was given in evidence;
(g) the number of offences in respect of which convictions were recorded; and
(h) the total expenditure (including expenditure of a capital nature) incurred by the agencies in connection with the execution of warrants.

Supervisory authority

8.32 The Australian legislation does not establish its own supervisory authority. Instead, it confers the review function on the Commonwealth Ombudsman. Unlike the Commissioner for Administrative Complaints in Hong Kong, the Australian Ombudsman has the power to investigate complaints against the Federal Police. He has accordingly in his general role investigated complaints alleging various forms of misconduct such as harassment and misuse of personal information.[21] Clearly this role does not restrict him to the investigation of *authorised* interceptions as in the case of the Commissioner of Interception of Communications in the United Kingdom.

8.33 Under the Telecommunications (Interception) Act 1979, the Ombudsman has the additional specific function of inspecting government records at least twice annually to ascertain compliance with reporting requirements and the destruction of intercepted materials. For the purposes of such an inspection, he has powers to enter premises and be furnished with records. He also has powers to obtain information from officers of the agency.[22] These investigative powers resemble those conferred on the Privacy Commissioner for Personal Data and the Commissioner for

19 *Ibid*, section 97.
20 *Ibid*, sections 99 - 104.
21 See the chapter on "Ombudsman" in G A Flick, *Federal Administrative Law* (1984), vol 2.
22 *Op cit*, sections 82 - 92.

Administrative Complaints in Hong Kong and are absent from the United Kingdom Interception of Communications Act 1985.

Remedies

8.34 Civil remedies are available to an aggrieved person in both civil and criminal proceedings. Where a person has intercepted a communication passing over a telecommunication system in contravention of the 1979 Act, the court may, in both civil and criminal proceedings, grant the aggrieved person remedial relief by making an order of one or more of the following kinds:[23]

(a) a declaration that the interception is unlawful;
(b) an order for damages against the defendant or accused (damages may be punitive in nature);
(c) an order in the nature of an injunction;
(d) an order that the defendant pay an amount not exceeding the gross income derived from the interception.

THE OPTIONS

8.35 Having considered the position in the three selected jurisdictions, we examine in the remaining paragraphs the various options for monitoring the implementation of the warrant system. The remedies available to an aggrieved individual will also be covered.

Supervisory Authority

8.36 Whereas the United Kingdom and Australia have a specially constituted administrative body tasked to monitor the application of the warrant system, the relevant authority in the United States simply collates and publishes the data received. This parallels the respective countries' data protection regimes, with only the United States lacking a true supervisory authority.

8.37 The Australian Ombudsman is full-time (as are his subordinates) but interception of communications is only one of his office's concerns. The United Kingdom Commissioner is part-time but focuses solely on supervising interception of telecommunications and mail.

The need for a supervisory authority

8.38 A requirement that the object of interception be subsequently notified of that fact would reduce the need for an independent review.

---

[23] *Op cit*, section 107A.

Notification would equip the individual with explicit grounds to challenge the issue or application of the warrant. However, we have rejected a notification requirement and the issue of independent review therefore becomes crucial in maintaining public confidence in the system: as the individual will not be in a position to challenge the interception it is essential that another party can scrutinise the matter on his behalf. We therefore conclude that it is necessary to set up an independent supervisory authority to keep the warrant system under regular review.

Justice of Appeal as supervisory authority

8.39 The next question is whether an existing body could be utilised or a new body should be created. The two existing bodies that theoretically could play a role are the Commissioner for Administrative Complaints and the Privacy Commissioner for Personal Data. We note that in Australia the Ombudsman fulfils a supervisory function in relation to interception of communications. We do not favour such an approach in Hong Kong, however. It is clear that the Commissioner for Administrative Complaints in Hong Kong has a more restricted remit than his Australian counterpart. Significantly, the Hong Kong Commissioner is excluded from investigating complaints relating to the Police or the Independent Commission Against Corruption, or matters affecting "security, defence or international relations .... in respect of Hong Kong". The exercise of a supervisory function in relation to the interception of communications is clearly a matter of considerable sensitivity. The office of the Commissioner for Administrative Complaints was not established with that role in contemplation, and we do not think it would be desirable now to seek to tack that task on to the existing functions.

8.40 In contrast, the Privacy Commissioner's duties do have some nexus with the interception of communications, in that it would sometimes be apparent from personal data that they have been collected by means of an interception of communications. We conclude, however, that it would not be appropriate to involve the Privacy Commissioner in this distinct field of regulation. His role under the Personal Data (Privacy) Ordinance is essentially to ensure fair play in the processing of personal data. The role of reviewing the authorisation of interceptions is different, and no other jurisdictions confer this additional role on their privacy commissioners. That different spheres are involved is also suggested by the fact that, whereas data protection is the policy responsibility of the Secretary for Home Affairs, interceptions are a matter mainly for the Secretary for Security. Saddling the Privacy Commissioner with the role of reviewing the issue of warrants would significantly alter both the fact and the public perception of his present statutory role. The existing duties of the Commissioner will already prove taxing for an incumbent.

8.41 Furthermore, the person reviewing the issue of warrants will play a pivotal role in securing law enforcement and security interests and would require a high security clearance, unlike the Privacy Commissioner who may be denied access to very sensitive data under the Ordinance and whose

decisions are subject to appeal. Selecting an individual who satisfies both the data protection lobby and the law enforcement/security community would be difficult.

8.42 More fundamentally, we recommended above that warrants should be issued by a High Court judge, unlike the procedure in the United Kingdom where warrants are authorised by a minister. Any review of the propriety of a warrant's issue would necessarily also have to be carried out by a judge**,** albeit one who is more senior. This would mean that the supervisory authority would have to be a sitting or former judge of the Court of Appeal. Appointing a judge as the supervisory authority would have the benefit of having a person who is impartial, objective and incorruptible to monitor the system.

8.43 We envisage that the supervisory authority would be appointed by the Governor, on the recommendation of the Chief Justice.

8.44 **We recommend that -**

(a) a supervisory authority should be created to keep the warrant system under review;

(b) a sitting or former judge of the Court of Appeal should be appointed by the Governor, on the recommendation of the Chief Justice, as the supervisory authority; and

(c) the person appointed as the supervisory authority should hold office for a period of three years and should be eligible for reappointment for a further period of three years.

Jurisdiction of supervisory authority

8.45 The United Kingdom Commissioner for Interception is solely concerned with whether interceptions carried out pursuant to a warrant have complied with statutory requirements. The Commissioner accepts that if interception without the authority of a warrant were taking place, there would be no reason for such conduct to come to his attention.[24]

8.46 The Australian Commonwealth Ombudsman is not subject to this restriction and is entitled to investigate unauthorised interceptions. Nonetheless, he is not specifically tasked to endeavour to detect such interceptions, nor would he be equipped to do so.

8.47 We considered whether the supervisory authority should be empowered to investigate allegations not only of improperly issued warrants, but also of interceptions carried out without a warrant. We concluded that the supervisory authority should be restricted to investigating whether a warrant

[24] Lustgarten and Leigh, *op cit,* at 64.

had been properly issued and complied with. The authority would not itself be equipped to investigate whether unauthorised interceptions were occurring. Instead, such unauthorised interceptions would be a criminal matter for investigation by the police, rather than the supervisory authority.

Role and power of supervisory authority

8.48 The main control we envisage being undertaken by the supervisory authority would be checking that the reasons given in the affidavits supporting the issue of the warrant were genuine and that the warrant had been executed in accordance with its conditions. A warrant may not have been properly issued, either because the statutory provisions had not been properly applied, or because the supporting affidavits may be false.

8.49 We think that it should be left to the supervisory authority to determine which warrants he should examine and on what basis.

8.50 The supervisory authority should have power to examine any person who is able to give any information relating to his review. He should also be given access to such documents and information as he may require for the purpose of enabling him to carry out his functions.

8.51 The principles to be applied by the supervisory authority in reviewing the issue of a warrant should be those that are applied by a court on an application for judicial review.

8.52 **We recommend that -**

(a) the supervisory authority should have power to examine on his own initiative whether a warrant has been properly issued and whether the terms of a warrant have been properly complied with;

(b) the supervisory authority may -

(i) summon before him any person who is able to give any information relating to his review and examine that person for the purposes of such review;

(ii) administer an oath for the purposes of the examination under (i) above; and

(iii) require any person to furnish to him any information (on oath if necessary) and to produce any document or thing which relates to his review;

(c) the supervisory authority shall apply the principles applied by a court on an application for judicial review in reviewing the issue of warrants.

Comments of the Bar Association

8.53 We recommended in chapter 6 that warrants should be issued by a judge on an *ex parte* application. *Ex parte* applications are held in private and the party affected by the order does not have an opportunity of being heard. It is therefore a fundamental rule of practice in Hong Kong courts that any party affected by an *ex parte* order may apply to the court to discharge the order.[25]

8.54 The Bar Association commented that although the object of an interception may never discover that his communications have been intercepted, it is essential that an aggrieved party should have a right to apply to the High Court to set a warrant aside.[26] They explained that the application may be made to any judge of the High Court, but preferably to the judge who originally issued the warrant so that he can review his decision in the light of the arguments put forward by the aggrieved party. A decision on the application can then be the subject of an appeal to the Court of Appeal.

8.55 The Bar Association further suggested that the warrant may be set aside on one of the following grounds:

(a) the warrant was wrongly issued, in the sense that the applicant's evidence failed to establish the requisite criteria;

(b) there was material non-disclosure or misleading evidence by the applicant in obtaining the warrant;

(c) the requirements of the warrant have not been properly complied with.

8.56 Although we share the views of the Bar Association that a warrant should be set aside if one of the three grounds exists, we do not think the procedure envisaged by the Association is either feasible or practical. While a person may on rare occasions discover that his communications have been intercepted, there would be no way by which he could find out whether the interception had been carried out pursuant to a warrant. It would be inappropriate for the court to disclose, in response to a request made by an aggrieved person, whether or not a particular warrant had been issued; all information relating to the issue of a warrant must be kept confidential if the effectiveness of an interception is to be maintained.

8.57 We therefore conclude that an aggrieved person should not have a right to apply to the court to set a warrant aside. This conclusion, however, does not preclude us from considering whether the aggrieved person is entitled to complain to the supervisory authority if he believes that his communications have been unlawfully intercepted.

---

25 *H M S Archer* [1919] P 1, at 4.

26 Cf Rules of the Supreme Court (Cap 4, sub leg A), Order 32, rule 6.

Review at the request of an aggrieved person

8.58 Although interception is by its nature clandestine, there may be instances where a person discovers that his communications have been intercepted without his consent. For example, a person may notice that his mail has been opened by another person. Information relating to a telephone interception may also leak out accidentally during a trial.

8.59 We agree that any person who believes that his communications have been unlawfully intercepted should in principle have a right to request the supervisory authority to investigate whether there has been an unlawful interception. Since we have recommended that the supervisory authority should only have jurisdiction over interceptions authorised by the court, the main concern of the supervisory authority would be whether the statutory requirements relating to the issue of warrants have been breached.

8.60 **We recommend that an aggrieved person who believes that his communications have been unlawfully intercepted may request the supervisory authority to investigate whether there has been a contravention of the statutory requirements relating to the issue of warrants.**

Warrants which are still effective

8.61 Upon receipt of a complaint, the supervisory authority should first ascertain whether there is a warrant affecting the aggrieved person. If there is one which is still effective, he should refer the case to the High Court. A judge of the High Court (preferably the one who originally issued the warrant) should then review the case and decide whether the warrant has been properly issued and complied with.

8.62 The review should be conducted *ex parte*. In conducting the review, the judge may summon any person for examination and require him to furnish any information, document or thing that is relevant to the case.

8.63 Where the reviewing judge is satisfied that the warrant has been properly issued and complied with, he should affirm the warrant and notify the supervisory authority accordingly.

8.64 Where the judge concludes that the warrant has been improperly issued or complied with, he shall -

(a) set the warrant aside; and

(b) unless the intercepted material may be required for the purposes of establishing the illegality of the interception, order the destruction of the material.

8.65 After setting the warrant aside, the judge should refer the case back to the supervisory authority.

8.66 **We recommend that -**

(a) where the supervisory authority ascertains that there is a warrant affecting the aggrieved person which is still effective, he shall refer the case to the High Court;

(b) on referral of the case from the supervisory authority, a judge of the High Court (preferably the one who originally issued the warrant) shall review the case and decide whether the warrant has been properly issued and complied with;

(c) the review shall be conducted *ex parte* and the judge may examine any person and require him to furnish any information, document or thing that is relevant to the case;

(d) where the reviewing judge is satisfied that the warrant has been properly issued and complied with, he shall affirm the warrant and notify the supervisory authority accordingly;

(e) where the judge concludes that the warrant has been improperly issued or complied with, he shall -

(i) set the warrant aside; and

(ii) unless the intercepted material may be required for the purposes of establishing the illegality of the interception, order the destruction of the intercepted material;

(f) after setting the warrant aside, the judge shall refer the case back to the supervisory authority; and

(g) the decision of the judge who reviews the case on referral by the supervisory authority shall be final.

Warrants which have expired

8.67 Where the warrant in question has expired, there is no warrant that can be set aside by the High Court. In these circumstances, the supervisory authority himself should review whether the warrant had been properly issued and complied with. In conducting the review, the supervisory authority should have power to order the destruction of intercepted material if

the warrant had not been properly issued or complied with. As the decision of the supervisory authority is not a decision of a court, it is necessary that his decision shall be final and not be open to review.

8.68 **We recommend that -**

(a) where the warrant affecting the aggrieved person has expired, the supervisory authority shall review whether the warrant had been properly issued and complied with and will have the same power as a judge in dealing with the intercepted material; and

(b) any decision of the supervisory authority shall be final.

Notification to aggrieved person

8.69 Where the reviewing judge has set aside a warrant, or the supervisory authority concludes that the warrant had not been properly issued or complied with, the supervisory authority should notify the aggrieved person that there has been a contravention of the statutory requirements relating to the issue of warrants.

8.70 In any other case, that is where -

(a) the supervisory authority ascertains that there is no warrant affecting the aggrieved person; or

(b) the warrant is affirmed by the reviewing judge; or

(c) the warrant has expired and the supervisory authority concludes that it had been properly issued and complied with,

the supervisory authority should refrain from making any comments other than informing the aggrieved person that there has been no contravention of the statutory requirements relating to the issue of warrants.

8.71 It would be inappropriate to notify the aggrieved person that the interception was conducted in accordance with a properly issued warrant because this would run the risk of rendering any on-going investigation futile - the suspect may have connections with the aggrieved person or he may be the aggrieved person himself. By the same token, the aggrieved person should not be notified that there is no warrant in existence if this was the case, because doing so would provide a suspect with a backdoor to verify whether he has or has not been a target of the law enforcement agency.

8.72 Equally important is the timing of any response to a request from an aggrieved person. Too prompt a response may enable the aggrieved person to deduce whether an intercept is, or is not, in place. We note that this is a matter which will require consideration by the Administration or the supervisory authority.

8.73 On notification of the finding that there has been no contravention of the statutory requirements, the aggrieved person would infer that the interception, if any, is either lawful (in the sense that it was authorised by the court) or unlawful (in the sense that it was carried out without court authorisation). If he is dissatisfied with this finding, he may report the matter to the police for further investigation. It is open to the police to mount a prosecution provided that there is enough evidence to prove that the interception was unlawfully carried out.

8.74 **We recommend that -**

(a) where the reviewing judge has set aside a warrant or the supervisory authority concludes that the warrant had not been properly issued or complied with, the supervisory authority shall notify the aggrieved person that there has been a contravention of the statutory requirements relating to the issue of warrants;

(b) in any other case, the supervisory authority shall refrain from making any comments other than informing the aggrieved person that there has been no contravention of the statutory requirements relating to the issue of warrants.

Notification delayed if prejudice to investigation

8.75 Although the aggrieved person should be notified if there has been a breach of the statutory requirements relating to the issue of warrants, notification may be delayed if it would seriously hinder the investigation of serious crime or prejudice the security of Hong Kong. One example would be where the irregularity has been remedied by the issue of a new warrant replacing the original one. The interception or investigation may continue for some time after the original warrant has been set aside. Informing the aggrieved person prematurely would frustrate the gathering of intelligence to be obtained from the interception which is now in all respects lawful. Even if the original warrant was not replaced by a new one, notification may still be withheld if this would affect existing or future investigation, whether such investigation relates to the aggrieved person or not. The supervisory authority should therefore have power to delay notification if he is satisfied that this would seriously hinder existing or future investigation of serious crime or prejudice the security of Hong Kong. The delay should, however, be no longer than is necessary. The supervisory authority should keep the case under regular review and notify the aggrieved person of the result as soon as the reasons for the delay are no longer effective.

8.76 **We recommend that the supervisory authority should have power to delay notification if he is satisfied that this would seriously hinder existing or future investigation of serious crime or prejudice the security of Hong Kong.**

Compensation to the aggrieved person

8.77 Given that both the warrant application and the interception were carried out by the authorities in secret, the aggrieved person would have difficulty in seeking legal remedy if he suffers any loss by reason of a breach of the statutory requirements. In order to protect the secrecy of interception activities carried out by the law enforcement agencies, the aggrieved person would simply be notified of the existence of a breach; he would not be informed of the reasons for coming to that conclusion. He would therefore have an impossible task in securing enough evidence to prove that there had been an unlawful interception and that he had been the object of that interception. Due to the sensitivity of the matter, the authorities would also be reluctant to disclose the details of the application and other relevant confidential material in open court. It is therefore impractical to ask the aggrieved person to seek compensation by taking civil proceedings.

8.78 In order to provide a practical and effective remedy for the aggrieved person, the supervisory authority should have power to award compensation to the aggrieved person if the authority concludes that the warrant has been improperly issued or complied with, or if the warrant has been set aside by the judge. That compensation would be paid out of public funds. We think it right that before reaching any conclusion on the question of compensation, the supervisory authority should give the aggrieved person an opportunity to be heard on this issue. An alternative to the approach we favour would be to establish a separate tribunal to consider the issue of compensation. This would have the advantage of separating the two functions of supervision and recompense, but we do not believe that the volume of likely work justifies the administrative costs of establishing a separate tribunal, nor that such a tribunal would provide any significant advantage over our proposal to leave the task of assessing compensation with the supervisory authority.

8.79 We believe that any loss suffered by the aggrieved person, including any injury to his feelings, would be adequately compensated by such compensation as may be awarded by the supervisory authority. To avoid re-opening issues in court proceedings, the aggrieved person should not be allowed to claim damages in court if he has already been awarded compensation by the authority. This is not to deny the right of an aggrieved person to seek legal remedies. On the contrary, our proposal takes account of the practical difficulties of an individual in claiming damages by bringing a legal action of his own. We believe that compensation awarded by the supervisory authority would provide a far more practical and effective redress to the aggrieved person without at the same time compromising the secrecy and effectiveness of the interception activities.

8.80 **We recommend that -**

(a) the supervisory authority should have power to pay compensation to the aggrieved person out of public funds if the authority

concludes that the warrant has been improperly issued or complied with, or if the warrant has been set aside by the reviewing judge;

(b) the aggrieved person should not be allowed to claim damages in court if he has already been awarded compensation by the supervisory authority.

Referral to Attorney General

8.81 **We recommend that where there is evidence suggesting that a crime has been committed by the applicant in obtaining the warrant or by the person executing the same, the supervisory authority may refer the matter to the Attorney General to consider whether to bring criminal proceedings against the offender.**

Reports

8.82 All three jurisdictions discussed above endorse a degree of transparency about interception activities. This is achieved by publishing statistics on the number of warrants issued, which is the only data provided by the United Kingdom Commissioner's annual report. The Commissioner has repeatedly said that the number of warrants is a misleading guide to the number of lines intercepted, but has declined to indicate the number of people affected.[27] The statistics are widely thought to understate the position (e.g. the Act allows one warrant to authorise the interception of communications to or from any number of addresses). The lack of detail on other matters lends scope for manipulation of the figures. By way of contrast, the United States reports give a detailed (and graphic) picture of the incidence, cost, and effectiveness of interceptions engaged in for law enforcement purposes. Those engaged in such intrusions are accordingly accountable.

Public reports to the Legislative Council

8.83 In the previous chapter we argued that the main benefit of a notification requirement is that it increases accountability. We rejected such a requirement for practical reasons. However, detailed annual reports provide an alternative method of achieving accountability. We believe that reports play a crucial role in increasing public accountability for intrusive activities carried out by the Administration and its law enforcement agencies.

8.84 **We recommend that the supervisory authority should furnish annually a public report to the Legislative Council.**

---

[27] Lustgarten and Leigh, *op cit,* at 60.

8.85 Unlike section 8 of the United Kingdom Act, however, we prefer to specify the different matters which must be included in the report. The United States report focuses on the cost effectiveness of interceptions, but in our view this cannot be assessed in purely financial terms. Interceptions are becoming increasingly cheap and the more relevant factor is that of the degree of intrusion into the individual's privacy.

8.86 **We recommend that there should be a statutory requirement that the following matters be covered by the report to be furnished by the supervisory authority:**

(a) the number of warrants applied for, withdrawn, rejected, granted as requested and granted subject to modifications;

(b) the average length of warrants and their extensions;

(c) the classes of location of the place at which communications were to be intercepted, e.g. domestic, business etc.;

(d) the types of interception involved, e.g. interception of telecommunications, interception of mail, etc.;

(e) the major categories of serious crime involved;

(f) statistics relating to the effectiveness of interception in leading to the arrest and prosecution of those charged with serious crime;

(g) the number of reviews conducted by the supervisory authority in response to a request by an aggrieved person, and an overview of such reviews; and

(h) the findings and conclusions of the review conducted by the supervisory authority in respect of the application of the warrant system.

8.87 The supervisory authority would not be required to provide the technical details of the interceptions. Under item (c), all he has to mention in the report is a general classification of the location of the place at which communications were to be intercepted, for example,. whether the interceptions were targeted at residential or commercial premises.

8.88 As regards (f), the consultation paper recommended that the reports should include the number of persons arrested and convicted as a result of the interceptions. One respondent commented that it may be difficult to draw up any accurate correlation because of the gap in time between the gleaning of intelligence, arrest, prosecution and conviction. Further, it would

not be possible to establish the number of persons convicted "as a result" of the interception. Any figures appearing in the report would be misleading.

8.89 We acknowledge the difficulties envisaged by the respondent if the authorities were required to indicate how many arrests and convictions were a direct consequence of interceptions. We have accordingly revised the recommendation such that the reports would only need to present statistics relating to the effectiveness of the interceptions in *leading to* arrests and prosecutions. These statistics are important because they will indicate the yield of the interceptions and will make the authorities accountable to the community regarding their utility. If large scale interception led to few arrests or prosecutions, the community would be entitled to question whether interception is an effective means in combating serious crime and whether the interference with privacy is justified by the results. We believe the reference to prosecutions instead of convictions would more accurately reflect the effectiveness of warrants because the result of a prosecution is contingent on many factors which have no direct bearing on the utility of interceptions. In order to find out how effective the warrants are, the authorities should provide information on the proportion of cases for which warrants had been issued that led to an arrest or prosecution within a specified period of time (e.g. two years).

8.90 Initially we were disposed to agree that the number of persons whose communications had been intercepted and the number of communications intercepted should be included in the report. However, information on the number of persons whose communications had been intercepted cannot be provided because it is not always possible to identify the parties to a telephone conservation simply by listening to the conversation, and information on the number of communications intercepted does not serve any useful purpose. We think that the particulars we have recommended above should sufficiently reflect the degree of privacy intrusion in society.

8.91 The Hong Kong Journalists Association proposed that the public report should include a section on "warrants issued to monitor communications by media outlets". We believe that media and non-media should be treated alike. If the report were to make special reference to media communications, it would be possible to argue that reference should also be made to the interception of communications with legislators, senior officials, judges and so forth. We stress that the warrant procedure would be under the control of High Court judges and not Government officials as in the United Kingdom. Such a system should secure public confidence.

8.92 We are advised by the Judiciary Administrator that the Chief Justice has expressed reservations on our proposal as to reporting requirements. The Judiciary Administrator pointed out that the idea of a Justice of Appeal submitting a report to the Legislative Council which will then be subject to the Legislature's scrutiny is undesirable and would blur the separation between the Judiciary and the Legislature. We agree that it is important to maintain the independence of judges and the Judiciary.

However, the Justice of Appeal concerned would not be acting in a judicial capacity when discharging the functions of the supervisory authority. He would be performing an administrative function when reviewing the issue or execution of warrants and investigating complaints from aggrieved individuals. We do not believe that there is any question of our proposal undermining the independence of the Judiciary. In the United Kingdom, the Commissioner appointed under the Interception of Communications Act 1985 is a senior judge. He is under a duty to make a report to the Prime Minister with respect to the carrying out of his functions. Upon receipt of the report, the Prime Minister will table it before each House of Parliament. There is apparently no difficulty with the idea of a judge making a report to Parliament via the Executive if he is not acting in a judicial capacity.

Confidential reports to the Governor

8.93 In discharging his review function, the supervisory authority may discover irregularities, the reporting of which would be prejudicial to the prevention or detection of serious crime or to the security of Hong Kong. Although such information ought not be disclosed in the public report, it should be made available to the Governor by means of a confidential report submitted by the supervisory authority.

8.94 The confidential report should cover such matters as are required by the Governor, or considered relevant by the supervisory authority. For instance, information on particular segments of the population being targeted might be considered relevant.

8.95 **We recommend that the supervisory authority should furnish annually a confidential report to the Governor. The report should cover such matters as are required by the Governor, or considered relevant by the supervisory authority.**

Reports by the Telecommunications Authority and telecommunication and mail service providers

8.96 In order to assist the supervisory authority in carrying out his functions, the licensed telecommunications carriers should be required to submit quarterly reports to the Telecommunications Authority with respect to the provision of telecommunication facilities for the purpose of enabling telecommunications to be intercepted under a warrant. Upon receipt of such reports, the Telecommunications Authority should pass them on to the supervisory authority for information.

8.97 **We recommend that all licensed telecommunications carriers should be required to furnish quarterly reports to the Telecommunications Authority for onward transmission to the supervisory authority. The quarterly reports should provide information relating to the following matters:**

(a) acts done by employees of the licensed carriers to assist the interception of telecommunications under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the average length of time during which telecommunications were intercepted under warrants which have expired within the reporting period.

8.98 We think that a similar obligation should be imposed on the Post Office, the Customs and Excise Service and the courier companies with respect to postal mail.

8.99 **We recommend that the Post Office, the Customs and Excise Service and the courier companies should furnish quarterly reports to the supervisory authority containing the following matters:**

(a) acts done by their employees to assist the interception of postal mail under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the total number of items intercepted.

8.100 The reports furnished by the courier companies may be routed through the licensing system for mail.

Operational implications

8.101 In the case of *Preston*, it was pointed out that:

> *"Those who perform the interceptions wish to minimise the dissemination of the fact that they have been performed, since it is believed that this would diminish the value of activities which are by their nature clandestine."*[28]

> *"[The] purpose of s. 9 [of the United Kingdom Act is] the protection, not of the fruits of the intercepts, but of information as to the manner in which they were authorised and carried out. ... the defendant was not to have the opportunity to muddy the waters at a trial by cross-examination designed to elicit the Secretary of State's sources of knowledge or the surveillance authorities' confidential methods of work."*[29]

---

28 [1993] 4 All ER 638 at 648.

29 *Ibid,* at 667.

8.102 Even accepting the rationale of this approach, we do not think that publication of informative reports such as we propose above will "diminish the value" of interception activities. Since the figures to be published in the report will be anonymised, it cannot be argued that their publication could prejudice the purposes of the original intrusion in particular cases. We would question the claim that the dissemination of even general data could have adverse consequences, but in any event consider that considerations of accountability should prevail. We believe that the public should know the extent of interceptions in their society.

Civil remedies

8.103 In our view, the United Kingdom's provisions for monetary compensation[30] are illusory. They are restricted to breaches of statutory requirements in the issue of warrants. A person who suffers loss by reason of an unauthorised interception cannot claim any compensation under the Act. Not surprisingly, no compensation has been awarded to date by the specially constituted tribunal. In contrast, both the United States and Australian laws provide aggrieved parties with a statutory right to claim in court monetary recompense for unauthorised interceptions.

8.104 For the reasons given above, we doubt the feasibility of the supervisory authority's investigating whether an unauthorised interception has been conducted. Nonetheless, whilst it would be unusual for an individual to learn that he had been subject to unauthorised interceptions, this may happen from time to time.

8.105 In particular, we recommended that a person who believes that his communications have been unlawfully intercepted may request the supervisory authority to investigate the matter. Under our proposals, the aggrieved person will be notified if there has been a contravention of the statutory requirements relating to the issue of warrants. If he suffers any loss as a result of the breach, he will normally have the right to claim compensation by taking civil action in court.

8.106 Another situation where an aggrieved person may become aware of an unlawful interception is when criminal proceedings are brought against a person who is in breach of the law regulating the interception of communications. For example a private detective who is found to have intercepted a telephone conversation may be prosecuted for committing the interception offence. The victim should be able to sue the private detective for damages if he suffers any loss.

8.107 However, for reasons given earlier, we do not consider the aggrieved person should be allowed to claim damages in court if he has already been awarded compensation by the supervisory authority. We

[30] Interception of Communications Act 1985, section 7(5)(c).

therefore conclude that a person who intercepts a communication unlawfully should be liable to compensate the aggrieved party for any loss suffered by him as a result of the unlawful interception unless the aggrieved party has been awarded compensation by the supervisory authority. In addition to damages for actual loss suffered there should, in line with the Personal Data (Privacy) Ordinance,[31] be compensation for injury to feelings.

8.108 **We recommend that any person who intercepts a communication unlawfully should be liable to pay compensation to the person who suffers damage by reason of the unlawful interception unless the latter has been awarded compensation by the supervisory authority. Damage should be defined as including injury to feelings.**

8.109 We have considered whether the intruder should be liable to pay punitive damages. Punitive damages represent a windfall to the aggrieved party because he may already have been compensated for his actual monetary loss and injury to his feelings. Nonetheless, this would be an appropriate remedy where the intruder has profited from his own wrongdoing.

8.110 **We recommend that the remedy to be granted by a court in a civil action for unlawful interception may include an order requiring the defendant to pay punitive damages to the aggrieved party.**

Supervisory tribunal

8.111 In addition to establishing a supervisory authority, section 7 of the United Kingdom Act establishes an independent tribunal to investigate complaints regarding the issue of warrants. A person who believes that he was the object of interception may apply to the Tribunal for an investigation of whether a warrant has been issued and, if so, whether this has been done in accordance with the Act. The jurisdiction does not extend to unauthorised interceptions; under section 1 that is a criminal offence and its investigation is therefore a matter for the police.

8.112 Our reasons for concluding that it is not feasible for the supervisory authority to investigate unauthorised interceptions apply equally to a complaints tribunal. Furthermore, we have recommended that the supervisory authority be empowered to pursue complaints and that aggrieved individuals be able to pursue claims for compensation in the courts. For these reasons, we do not consider that a separate complaints tribunal will be required to supplement the role of the supervisory authority.

[31] Section 66(2).

Chapter 9

The interception of Communications by the media

Summary

9.1 *We examine the view that journalists should be allowed to use intrusive techniques to infringe an individual's right to privacy whenever the disclosure of information obtained by such means can be justified in the public interest. The principles underlying the freedom of the press and the right to seek and receive information are explored and their relevance to a general prohibition of interception of communications considered.*

9.2 *We are of the opinion that the means of news-gathering and the disclosure of information obtained by such means are two separate issues which should not be confused. The media should always gather news by fair and lawful means. That is the case even though the information to be obtained can be disclosed in the public interest.*

9.3 We conclude that our proposals in this report neither impinge on the freedom of the press nor on the freedom of information and that the media should not be exempted from the regulatory framework.

Response to the Consultation Paper

9.4 Some of those who commented on the sub-committee's consultation paper argued that its proposals would infringe the public's right to know and the right to receive information. They pointed out that normal journalistic activities should not be subject to prior censorship and a balance should be maintained between the right to privacy and the freedom of the press. It should, however, be borne in mind that the consultation paper covered both surveillance and the interception of communications. Most of the concerns of the media relate to surveillance, a term which has a wide meaning in the consultation paper, as opposed to the interception of communications.

9.5 The Hong Kong Journalists Association argued that the warrant system would give the judges a power to decide what should be subject to

journalistic inquiry. They added that if the sub-committee's proposals were adopted, the media would have difficulties in monitoring the performance of the government.

9.6 A few respondents expressed the view that journalists should be permitted to use intrusive techniques to invade an individual's privacy whenever the disclosure or publication of the information obtained by such means could be justified in the public interest. They were in effect arguing that the end should justify the means. We shall explain below that the issues of intrusion and disclosure are separate and should not be confused.

The right to seek and receive information

9.7 Article 19 of the ICCPR acknowledges that everyone has the freedom to seek and receive information.[1] Paragraphs 2 and 3 of the article state:

> *"2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) for respect of the rights or reputations of others;*
> *(b) for the protection of national security or of public order (ordre public), or of public health or morals."*

9.8 The term "seek" was adopted instead of "gather" in order to protect active steps to procure and study information. It was thought that any abuse of the freedom to seek information would be addressed by paragraph 3 of the article.

9.9 It should be stressed that article 19 does not impose a duty on any person to disclose information which he is reluctant to disclose, nor does it entitle a person to extract information from an unwilling speaker.[2] Nowak explains:

> *"The right to seek information in any event relates to all generally accessible information. In the context of personal data and other specific information on a person, it is possible to assume that the individual concerned has a farther-reaching*

---

1 I.e. Hong Kong Bill of Rights, article 16.

2 See E Barendt, *Freedom of Speech*, (Oxford: Clarendon Press, 1987), chapter III.5.

> *right to be informed of such data, insofar as this is not opposed by pressing interests of secrecy on the part of the State or the private data bank. It is, however, debatable whether the public mandate on the press and electronic media to inform the public truthfully of all events of interest implies a privileged right of journalists to seek information above and beyond that which is generally accessible."*[3]

9.10 The freedom of information is not absolute. Article 19(3) provides for restrictions on this freedom to protect the rights of others. Nowak comments:

> *"[The] freedom to seek information may be limited in the interest of the rights of others. Principally conceivable here is the protection of privacy and intimacy pursuant to Art. 17. Even though the drafters of Art. 19 expressly adopted the right to seek information actively, this does nothing to change the duty on States Parties flowing from Art. 17 to protect the intimacy of the individual against sensational journalism. Above all, the legislature must prevent abusive access to personal data."*[4]

9.11 The European Convention on Human Rights contains a right to "freedom to receive and impart information and ideas without interference by public authority".[5] The right to receive information envisages access to general sources of information only. It is not clear whether, and if so to what extent, the freedom to receive information entails an obligation on the part of the public authorities to impart information.[6] It appears that this right is nothing more than a liberty to receive information imparted by a *willing* speaker.

The freedom of the press[7]

9.12 Although neither the ICCPR nor the European Convention makes any provision for freedom of the press, that concept forms part of the freedom of expression and information under both treaties.[8]

---

3 M Nowak, *UN Covenant on Civil and Political Rights - CCPR Commentary* (1993), at 343.

4 *Ibid*, at 354.

5 Article 10.

6 See P van Dijk & G J H van Hoof, *Theory and Practice of the European Convention on Human Rights* (The Netherlands: Kluwer Law and Taxation Publishers, 1990), at 417-418. The European Court of Human Rights held that "the right to freedom to receive information basically prohibits a government from restricting a person from receiving information that others wish or may be willing to impart to him. Article 10 does not confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the government to impart such information to the individual". See *Leander v Sweden* (1987) 9 EHRR 433, paragraph 74.

7 On freedom of the press, see generally E Barendt, *Freedom of Speech*, (Oxford: Clarendon Press, 1987), chapter II.6; G Robertson & A Nicol, *Media Law*, (Penguin, 3rd ed, 1992), chapter 1.

8 Article 27 of the Basic Law provides that Hong Kong residents will have "freedom of speech, of the press and of publication".

9.13 The Third Royal Commission on the Press in the United Kingdom defines freedom of the press as -

> *"that degree of freedom from restraint which is essential to enable proprietors, editors and journalists to advance the public interest by publishing the facts and opinions without which a democratic electorate cannot make responsible judgments."*[9]

9.14 The freedom of the press may mean the freedom of individuals (including journalists) to publish information and opinion through the press without prior restraint. This freedom may entail the freedom of proprietors to market their publications and the freedom of editors to decide what shall be published. The claims that the media should be independent of the state and that speakers should have access to the means of communication are other aspects of press freedom.

9.15 While article 19(3) provides that the exercise of the right to freedom of information "carries with it special duties and responsibilities", the English Court of Appeal in *Francome* emphasised that proprietors and journalists are not above the law:

> *"Parliamentary democracy as we know it is based upon the rule of law. That requires all citizens to obey the law, unless and until it can be changed by due process. There are no privileged classes to whom it does not apply. If ... the Daily Mirror can assert this right to act on the basis that the public interest, as he sees it, justifies breaches of the criminal law, so can any other citizen. This has only to be stated for it to be obvious that the result would be anarchy."*[10]

The United States approach

9.16 Both the Hong Kong Journalists Association and the Hong Kong News Executives Association claimed that the United States choose to deal with the issue of privacy by the law of tort in civil law. This is inaccurate. The media in the United States are subject to the provisions of the Wiretap Act in the same way as any other ordinary individuals. The United States Supreme Court has held that the First Amendment to the United States Constitution "has never been construed to accord newsmen immunity from torts or crimes committed during the course of news-gathering. The First Amendment is not a licence to trespass, to steal, or to intrude".[11]

9.17 As explained by Emerson, although the press in the United States has a right to obtain information from private sources on a voluntary basis, it has no power under the constitution to compel the production of such

---

9 Royal Commission on the Press, *Final Report*, (Cmnd 6810, 1977), paragraph 2.3.

10 *Francome v Mirror Group Newspapers* [1984] 2 All ER 408, at 412.

11 *Dietemann v Time*, 449 F 2d 244, 249 (9th Cir 1971). The First Amendment provides for a constitutional guarantee of freedom of the press.

information.[12] Whereas the rule against prior restraint is relevant where an injunction is sought against *publication* of information, there is no infringement on the freedom of the press if an injunction is sought against unlawful *intrusion* upon privacy by the press.[13]

Privacy intrusion *vs* disclosure or publication of personal information

9.18 We have mentioned that some of those who commented on our consultation paper argued that physical intrusion by the media should not be prohibited where the publication of the information obtained in consequence of the intrusion is in the public interest.

9.19 We agree that the defence of public interest may be relevant in resolving the issue of disclosure or publication.[14] However, the act of intrusion itself, as distinct from disclosure, is a different matter. In the United States, the media would be liable for employing intrusive means to obtain information even though they may rely on the defence of newsworthiness in an action for disclosure of private facts collected by such means. As pointed out by Wacks, none of the justifications for free speech which form the basis of the First Amendment protection of disclosure apply to intrusions upon privacy.[15]

9.20 It is important to distinguish between the means of news-gathering and the consequences which flow from such activities.[16] The media has always been subject to limitations imposed upon news-gathering methods by the laws of trespass, copyright, theft, fraud, criminal damage and other like offences under the criminal law. There has never been any suggestion that such limitations infringe upon the freedom of the press, or the freedom to seek or receive information.

9.21 Just as an ordinary citizen cannot search a person or break into a house in order to obtain information the publication of which may be justified in the public interest, so no journalist should be allowed to intercept a private communication merely because the publication of the information to be obtained by the interception is justified in the public interest. The publication of information, and the means of obtaining the information, should

---

12 T Emerson, *The Right to Privacy and Freedom of the Press*, (1979) Vol 14, No 2, Harv CR-CLLR 329; collected in R Wacks, *Privacy Volume II - The Concept of 'Privacy'* (London: Dartmouth, 1993) 375.

13 *Galella v Onassis*, 487 F 2d 986 (2d Cir 1973).

14 E.g. where a person obtains information by intrusive means and subsequently discloses the information in breach of his duty of confidence, he may rely on the defence of public interest in an action for breach of confidence.

15 R Wacks, *Privacy and Press Freedom* (London: Blackstone Press, 1995), at 127. The following are some of the arguments which are commonly advanced to justify the protection of the freedom of speech: (a) dissemination of information and opinion; (b) facilitating exchanges between individuals and groups; (c) ascertainment of truth; (d) individual self-development and fulfilment; (e) participation in the working of democracy; and (f) facilitating social change.

16 See R Wacks, *Privacy and Press Freedom* (London: Blackstone Press, 1995), chapter 5.

always be kept separate and distinct. This is also the approach adopted in the Personal Data (Privacy) Ordinance.

News-gathering by fair and lawful means

9.22 The exemptions available to the media under the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) only relate to the *use* of personal data and the right of a data subject to have access to his personal data.[17] Nowhere can we find a provision in the Ordinance exempting the media from the "collection limitation principle" under data protection principle 1. Journalists, just as any other citizens, must collect personal data by means which are both *lawful* and *fair* in the circumstances. A person who adopts unlawful or unfair means to collect personal data cannot avoid the censure of the Privacy Commissioner by arguing that the publication of the data is in the public interest.[18]

9.23 We have made no proposals restricting what the media may publish. The media would continue to be free to publish anything which was legal. There is therefore no question of prior restraint upon publication.

9.24 Our report applies only to the *means* adopted by the media in news-gathering. We argue above that interception of communications is a serious invasion of privacy. We have therefore recommended that interception of communications should be made unlawful unless it is exempted or authorised by the court. Although the media would not be allowed to apply for an interception warrant under our proposals, they may still employ other less intrusive means, or rely on the exception applicable to consensual interception. Furthermore, the public will continue to enjoy the right to receive information obtained by fair and lawful means. As far as news-gathering activities are concerned, the freedom of the press is the freedom to gather news by fair and lawful means; it is not a freedom to gather news by means which are unlawful or unfair.

9.25 Intercepting a communication without the consent of any party to the communication is unfair and should be censured. Even if our proposals were not adopted, one would be very surprised if the Privacy Commissioner rules that the interception of communications without consent is a fair means of collecting personal data. Our proposals merely go one step further and recommend that unauthorised interception of communications is not only unfair but also unlawful.

9.26 It is beyond doubt that the press in Hong Kong enjoys a high degree of freedom. They are not subject to any licensing controls. The registration of a local newspaper under the Registration of Local Newspapers Ordinance (Cap. 268) is purely a matter of formality. The registration fee is minimal and there are basically no restrictions on who can own a newspaper.

---

17 Section 61. The term "use", in relation to personal data, is defined as including disclosure or transfer of data: section 2(1).

18 Cf section 61(2)(b).

If the interception of communications by the media were exempted from regulation, anyone, including criminals, who wanted to intercept a communication could take advantage of this exemption simply by registering as a newspaper proprietor. This is not something we would like to see. The alternative would be a licensing system for the press but this is clearly not in the interests of press freedom. The conclusion must be that the press should enjoy no privilege in the gathering of news. This is perhaps the price they need to pay for not having any licensing controls imposed on them.

9.27 We conclude that our proposals would not impinge on the freedom of the press or the freedom of information and that the media should not be exempted from the regulatory framework.

Annexure

Respondents to the Consultation Paper

Government

Security Branch
Transport Branch
Independent Commission Against Corruption
Director of Administration

Legal Profession

Hong Kong Bar Association
Law Society of Hong Kong
Judiciary Administrator's Office
International Law Division, Attorney General's Chambers

Political bodies

Office of the Hon Emily Lau
Office of the Hon James To
Hong Kong Alliance of Chinese and Expatriates
Hong Kong Human Rights Commission
Liberal Democratic Federation of Hong Kong
Chairman, Hong Kong Progressive Alliance

Media

Hong Kong Journalists Association
Hong Kong News Executives' Association
Hong Kong Press Photographers Association
Television Broadcasts Ltd

Academics

Open Learning Institute of Hong Kong
Hong Kong Polytechnic University
Prof Wang, City University of Hong Kong
Prof Tucker, Monash University, Australia
Mr Stefaan Verhulst, Glasgow University
Prof Horibe, Hitotsubashi University

Overseas bodies

Human Rights and Equal Opportunity Commission, Australia
Office of the Information & Privacy Commissioner, British Columbia, Canada
Federal Ministry of the Interior, Germany
Office of the Privacy Commissioner, New Zealand
Data Protection Registrar, United Kingdom
National Council for Civil Liberties, United Kingdom

Others

Hong Kong Telecommunications Ltd
Mr Heung Shu-fai