THE LAW REFORM COMMISSION OF HONG KONG

PRIVACY SUB-COMMITTEE

CONSULTATION PAPER

PRIVACY: REGULATING SURVEILLANCE AND THE INTERCEPTION OF COMMUNICATIONS

This Consultation Paper has been prepared by the Privacy sub-committee of the Law Reform Commission. It does not represent the final views of either the Privacy sub-committee or the Commission, and is circulated for comment and criticism only.

The Privacy sub-committee would welcome submissions on the proposals contained in this Consultation Paper. You are invited to make your views known to the sub-committee, in writing, by 15 June 1996.

All correspondence should be addressed to:

The Secretary,
The Privacy sub-committee,
The Law Reform Commission,
20th Floor, Harcourt House,
39 Gloucester Road,
Wanchai,
Hong Kong.

It may be helpful for the Commission or the sub-committee, either in discussion with others or in any subsequent report, to be able to refer to and attribute comments submitted in response to this Consultation Paper. Any request to treat all or part of a response in confidence will, of course, be respected, but if no such request is made, it will be assumed that the response is not intended to be confidential.

The Law Reform Commission's Privacy sub-committee

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.

This is the second part of a reference to the Law Reform Commssion on Privacy which has been considered by the Commission's Privacy sub-committee. The members of the Privacy sub-committee are:

Hon Mr Justice Mortimer	***Justice of Appeal (Chairman)***
Dr John Bacon-Shone	***Director, Social Sciences Research Centre, University of Hong Kong***
Mr Don Brech	***Records Management International***
Mrs Patricia Chu	***Assistant Director (Family & Child Welfare) Social Welfare Department***
Mr A F M Conway	***Great River Corporation Ltd***
Mr Edwin Lau	***Assistant General Manager, Retail Banking, Hongkong & Shanghai Banking Corporation***
Mr James O' Neil	***Deputy Crown Solicitor (Lands & Works), Attorney General's Chambers***
Mr Peter So Lai-yin	***Deputy Commissioner of Police (Management) Royal Hong Kong Police Force***
Prof Raymond Wacks	***Head of Department of Law University of Hong Kong***
Mr Wong Kwok-wah	***Bureau Chief, Asia Times***
Mr Mark Berthold	***Consultant, Law Reform Commission (Secretary)***

*The members of the sub-committee wish to express their appreciation for the work of **Mr Mark Berthold**, secretary to the sub-committee, who was principally responsible for the research and writing of this consultation paper*

The Law Reform Commission of Hong Kong

Privacy sub-committee

Consultation Paper

PRIVACY: REGULATING SURVEILLANCE AND THE INTERCEPTION OF COMMUNICATIONS

CONTENTS

Chapter	
	Introduction
1	The regulation of physical surveillance
2	Interception of communications: technical aspects
3	Statutory regulation of communications
4	The legal protection of privacy of communications
5	Interception of communications: legal issues
6	The regulatory framework
7	Notification following termination of surveillance
8	Compliance enforcement: supervisory authorities and remedies
9	Legal and policy issues arising from the impact of encryption and other new technologies
10	Other approaches to regulating intrusions: licensing
11	Summary of recommendations
Annexure	Breach of confidence

Introduction

Terms of Reference

1. The Law Reform Commission Privacy sub-committee' 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 issues raised at (a) and (b) are 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 on 3 August 1995. This paper deals with (c) and (d).

3. The references to "intrusion by any means (whether electronic or other means)" and "the interception of communications" in the terms of reference should not be interpreted as suggesting a dichotomy: they overlap in some situations. For example, it is now possible to "read" e-mail by monitoring by remote means the radiation emitted by a word processor (the technology is described in detail later). This could be characterised as either falling under (c) or (d).

4. This paper makes frequent reference to new technologies impacting on privacy. It is not suggested that a regulatory framework should focus on such technologies. Regulation must be founded on general principles. Nonetheless, an awareness of new applications of technology provides a checking mechanism to confirm that any proposed regulatory framework is indeed apt to cover the various applications. As suggested by the example in the previous paragraph, a problem with the differentiation of legal controls according to whether the activity constitutes "intrusion" or "interception of communications" is that the proposed dichotomy may not adequately take account of some applications. This paper will use the general term "surveillance" when both intrusion and the interception of communications are being referred to.

Relationship with data protection

5. 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 surveillance focuses on protecting the individual at the stage when information is acquired about him, whether or not it is captured as recorded data.

6. 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]

Increased need for privacy in a networked world

7. There is an increasing need for privacy and security of telecommunications:

---

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

- The public is likely to become increasingly concerned about privacy as a result of the increased amount of personal information available on-line or by using the phone.

- An allied concern is that of the global marketplace: the increased use of communications systems by industry has increased the need for security of communications in such areas as banking and finance. Another concern is that of theft of proprietary information. Security is widely viewed as the key component for the continued success of the information super-highway.

- Proposals that limit privacy and security of communications will ultimately slow the development of advanced networks. 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."[2]

- Many such networks are now global. Internet is a good example. Electronic messages can now be sent between countries without going through embassies, secure satellite links, military networks, or postal services. International borders have become meaningless.

Interception of telecommunications and data protection

8. The 1992 Australian Telecommunications Authority (AUSTEL) report on Telecommunications Privacy points out that the telecommunications industry has such specific characteristics as its global nature, high infrastructure costs, and rapidly developing technologies. However, these features are shared to varying degrees by other industries. Similarly, the capture and use of personal data is not unique to that industry. AUSTEL observes that "using telecommunications means for conveying personal information does not by itself comprise an issue of telecommunications privacy". It accordingly recommends that measures to control the collection and use of personal data by means of telecommunications networks should accord with the data protection principles.

---

[2] *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.

9. 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 information content of the communication itself - the conversation or message.*

10. 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 (the material described at the first and second point above). He points out, however, that subscribers would not regard the conversation or message (the material described in the third point above) as being subject to collection.

11. In the Hong Kong context, upon collection, that data will be subject to the application of the data protection principles pursuant to the Personal Data (Privacy) Ordinance. Accordingly we see our remit in this part of the reference as developing protections against serious intrusions that are supplementary to the more general provisions of the Ordinance. Whilst the zone of protection is narrower than under the Ordinance, we correspondingly recommend that exceptions be much narrower than those under the Ordinance.

Industrial espionage

12. An initial question is whether our consideration of surveillance should cover industrial espionage. Although we are not addressing corporate privacy as such, our recommendations will entail some overlap. This is inevitable because the regulation of physical surveillance concerns surveillance of individuals in whatever capacity they are acting at the time, including as corporate agents. The regulation of telecommunications, on the other hand, may involve less overlap with corporate privacy, arising for instance where there is communication between two computers and comprising solely commercial data. Although not our focus, we do not consider it necessary for our recommendations to exclude such situations. Similarly, while we wish to emphasise the protection of communications between individuals rather than between machines as such, we recognise that in practice machines mediate personal communication, such as where voice is recorded and stored for subsequent transmission between voice mail machines.

The interests requiring protection from surveillance

13. A key word in the terms of reference is "privacy". In his comprehensive review, Professor Raymond Wacks concludes that "in spite of the huge literature on the subject, a satisfactory definition of ' privacy' remains as elusive as ever."[3] We set out in the following paragraphs some of the more influential definitions of "privacy."

14. 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."*[4]

15. Alan 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."*[5]

16. 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."*[6]

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

> *"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."*[7]

18. While the above formulations venture a definition of "privacy" or its elements, the Australian Law Reform Commission follows the more empirical approach suggested by McCloskey:[8]

---

3 Wacks, *op cit*, at 13.

4 JUSTICE, *Privacy and the Law* (1970), para 19.

5 Westin A F, *Privacy and Freedom* (1967), p 7.

6 *Report of the Committee on Privacy and Related Matter*, 1990, Cmnd 1102.

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

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

"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."

19. According to this approach, one firstly ascertains the ordinary language concept and, secondly, determines whether the "privacy interests" so encompassed should, as a matter of policy, be protected. Relevant to this latter inquiry are such factors as the requirements of International Covenant on Civil and Political Rights (the ICCPR) as replicated in the Hong Kong Bill of Rights Ordinance (Cap. 383).

Article 17 of the ICCPR

20. Article 17 of the ICCPR 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. "

21. In its general comment on this provision (which is replicated as article 14 of the Hong Kong Bill of Rights[9]), the United Nations Human Rights Committee makes the following points on the ICCPR:

- This right is required to be guaranteed against all such 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. "

[9] Cap 383, Part II.

22. 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."*[10]

23. Also relevant to the interpretation of article 14 of the Hong Kong Bill of Rights is the jurisprudence interpreting the similarly worded privacy provision of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("the European Convention"). 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 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."*

24. The first limb of article 8 is in virtually identical terms to article 17 of the ICCPR, both being 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 to privacy.

---

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

25. Article 14 specifically identifies as within the zone of protection family life, home, and correspondence. The ambit of these expressions is reasonably clear and would preclude surveillance of domestic premises. Also, as held in *Klass,*[11] "correspondence" encompasses all telecommunications. But in ascertaining the scope of protection for surveillance in other spheres, recourse must be made to the word "privacy". In contrast to article 14, 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 14[12] dealt with surveillance of the applicant's youthful participation in political activities. In her analysis, Louise Doswald-Beck concludes that the ruling of the European Commission of Human Rights in that case does appear to be premised on the assumption that individual secret surveillance other than telephone tapping "may well amount to an interference with private life".

26. 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 surveillance society

27. In *Undercover,* Gary Marx describes "a subtle and deep lying shift" in social control:

> *"As powerful new surveillance tactics are developed, the range of their legitimate and illegitimate use is likely to spread. Where there is a way, there is often a will. There is a danger of almost imperceptible surveillance creep."*[13]

> *"The new surveillance goes beyond merely invading privacy, as this term has conventionally been understood, to making irrelevant many of the constraints that protected privacy. Beyond the boundaries protected by custom and law, privacy has depended on certain (technically or socially) inviolate physical, spatial, or temporal barriers - varying from distance to darkness to doors to the right to remain silent. An invasion of privacy required crossing these barriers. With much of the new technology, many of them cease to be barriers."*[14]

> *"Like the discovery of the atom or the unconscious, new control techniques surface bits of reality that were previously hidden or didn't contain informational clues. People are in a sense turned inside out,*

---

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

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

13 Gary Marx, *Undercover : Police Surveillance in America* (1988), at 2.

14 *Ibid,* at 231.

and what was previously invisible or meaningless is made visible and meaningful. This may involve space-age detection devices that give meaning to physical emanations based on the analysis of heat, light, pressure, motion, odor, chemicals, or physiological process, as well as the new meaning given to visible individual characteristics and behaviour when they are judged relative to a predictive profile based on aggregate data."[15]

Surveillance technologies

28. What are these new technologies that obviate privacy barriers? Wasik describes the following examples:

"A wide range of electronic devices is now available to improve upon the traditional techniques of the industrial spy or eavesdropper. Micro-transmitters can be placed in rooms where sensitive information is to be discussed. Such transmitters are commonplace and easy to obtain. Most of them transmit continuously once installed but some can be activated and de-activated by remote signal. These transmitters are very difficult to detect by physical search since they are so small and may be concealed in furnishings, light fittings, desk equipment, behind pictures, or even plastered into a wall. Silent and invisible flashlight photography can be achieved in darkness and cameras can be adapted to focus and take pictures through minute holes drilled in walls or furniture. Laser beams generated from outside a building can be reflected off the window of a room in which sensitive information is being discussed. Because speech sound-waves cause the window pane to vibrate very slightly, it is possible to record a signal from the reflected beam and re-create the speech."[16]

29. This (incomplete) description of personal surveillance techniques should be taken in conjunction with techniques aimed at eavesdropping computer data:

"Unauthorised access to the information may be achieved by a number of methods. It may be read off a VDU linked to the computer where the data is stored, either by an unauthorised person gaining physical access to the computer itself, or by the implantation of a listening device, a remotely operated camera, or the recreation of the data from electromagnetic radiation emitted by the computer equipment. . . Or it may be obtained by an unauthorised user accessing the computer directly from long range, through hacking, reading the relevant information or transferring a copy of it to the accessor's own files."[17]

---

15 *Ibid,* at 207.

16 Wasik M, *Crime and the Computer* (1991), at 53.

17 *Op cit*, at 52-53.

30. The reference to recreating electromagnetic radiation is to a process that highlights the opportunites now afforded to eavesdrop:

> *"It is technically quite possible to 'read' from outside a building information currently being relayed through a computer system inside the building, using a television receiver connected to a video recorder, to pick up the electromagnetic radiation surrounding the computer. The data can then be recreated in readable text on the eavesdropper's monitor, and recorded. The radiation emitted by computers is known as Radio Frequency Interference or Electromagnetic Radiation (ERM). Mainframes and minicomputers emit ERM from all sides of the terminal, including the screen display, as well as from printed circuit tracks and internal wiring. Some cables, particularly those connecting VDUs, disk drives and printers, also emit the signals. Telex and facsimile are similarly vulnerable. The technology necessary to intercept ERM is similar to that used in television licence detector vans, and is relatively cheap and easy to assemble and operate. ERM can generally be picked up within a range of 200 metres, although occasionally further . . . As an espionage device computer eavesdropping is rather haphazard, since the eavesdropper has no way of determining what material will be intercepted, but there is always the chance that useful information will be obtained, perhaps data being entered into the computer prior to encryption. It may also be provide a means of obtaining access to passwords . . . The most effective interim solution appears to be to limit the emission of ERM, by radio frequency filtering techniques, or the shielding of equipment or parts of the building itself, so that it does not pass beyond the building and cannot be intercepted externally."*[18]

Counter-surveillance

31. The development of surveillance technologies has generated a small industry devoted to counter-surveillance. Generally undertaken by private investigators, the techniques used may include:[19]

- Technical sweeps listening for such indicators as electronic pulses, surges, and radio frequencies. A passive recording device turns itself on or off in response to the noise level in the room. By using a tone generator to create noise the bug will commence transmitting. This can then be sensed by a detector sensitive to the smallest electronic oscillation or transmission. Similarly, a device is 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.

---

[18] *Op cit*, at 46-47.

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

- Physical examinations which may literally require "tearing the place apart" are often a necessary supplement. For example, a remotely controlled transmitter may be operated by using a touch-tone pad and therefore will not be activated by a noise generator.

- Active countermeasures, such as deploying jamming equipment. For example, an ultrasonic microphone jammer will generate a high frequency tone above the range of normal hearing. Any conversations or other sounds being surreptitiously recorded within this cone of white noise will be an indecipherable high pitched sound. Another measure is the use of scramblers. A small device snaps over the headset of the telephone or cellular phone to scramble the voice. Decoding requires a similar device set to a pre-arranged code.

Use of surveillance devices in Hong Kong

32. In Hong Kong the control and licensing of surveillance equipment is governed by the Telecommunication Ordinance (Cap 106) and enforcement is not by the police but by the Office of the Telecommunications Authority (OFTA). However, OFTA has not received a complaint in the last 3 years. Nonetheless, 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" which can, for $8900, transmit a conversation a kilometre away.

The social dimension of surveillance

33. David Lyon argues that "the growth of electronic surveillance has thrown up questions about 'privacy' that ultimately can only be addressed in terms of some conception of personhood and human identity."[21] This is implicit in the human rights jurisprudence that is analysed below in the context of the application of the Bill of Rights. But Lustgarten and Leigh amplify the implicit social concerns:

> *"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. Imagine being unable to draw the curtain in your bedroom, so that others can see you naked at any time of their choosing. The fear and revulsion this image evokes has little to do with the beauty or otherwise of one's body, but everything to do with one's sense of <u>self</u>. If I have no control over*

---

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

21 David Lyon, *The Electronic Eye: the Rise of Surveillance Society* (1994), at 17.

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 ... . The promise that 'Big Brother is Watching You' derives its horror from the instinctive realisation that it means that one is someone else's subject, that in a figurative, but still meaningful sense, one is someone else's property.

As with the eye, so with the ear. 'Big Brother is Listening to You' is no less horrific. Clandestine interception or eavesdropping infringes upon a fundamental choice: with whom one chooses to speak. The only defences against it are silence and withdrawal. And here we reach the first point at which the individual character ... connects with the character of a society. 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. The knowledge, or even widespread belief, that one's words will be heard by someone other than those to whom one wishes to speak creates a society of timid, furtive creatures."[22]

34. To the suggested defences of "silence and withdrawal" we would add encryption. But the thrust remains that while serious social evils may be subject to surveillance, the exercise of the power of surveillance should be strictly limited. The undesirability of the development of a surveillance society had been earlier noted by the Younger Committee. It noted 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."[23]

Information warfare

35. It is also important to note, however, that the issue is not simply one of the State versus the individual. "Big Brother" may be part of the story, but its connotation that the State has a monopoly on surveillance is misleading. Further, much surveillance is conducted for purposes quite independent of the assertion of social control, or its defiance. For example, hacking is pursued for a variety of purposes ranging from curiosity, to profit, to disparate anti-social purposes.

Privacy technologies

36. The discussion so far assumes that technologies are invariably privacy invasive. This is an oversimplification. New technologies have been specifically developed

---

22 Lustgarten and Leigh, *In from the Cold: National Security and Parliamentary Democracy* (1994), at 39-40.

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

to *protect* privacy. Some of these technologies are based on the capability of concealing the identity of the data source. Anonymity is often the best means of securing privacy. Others, such as cryptography, scramble communication and thereby thwart interception efforts. However, it will be seen that some governments elsewhere are endeavouring to restrict the individual' s use of technologies designed to protect privacy.

The functional relationship between surveillance techniques

37. In *Undercover,* his seminal study of covert police work, Gary Marx provides a useful classificatory scheme according to whether surveillance is overt/covert and/or deceptive or non-deceptive. 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. From this vantage point, the investigation may be conducted not after the offence, as with overt police intervention, but before and during the commission of the offence. Nonetheless, undercover activities resemble covert or deceptive tactics in that they provide a means of discovering otherwise unavailable information.

38. Marx makes the important point that to the extent that controls are placed on overt and/or non-deceptive practices there will be an increased demand for covert and/or deceptive practices. Increased controls on unobtrusive surveillance will indirectly encourage the increased use of informer techniques. So if there is a warrant requirement for a bug or wiretap and approval is not forthcoming, undercover activities may be considered, particularly if such activities are legally unregulated. However, the two approaches may also be used together, with surveillance supporting undercover work by enhancing security (by facilitating intervention in emergencies), increasing accountability (by enabling verifications of agents' accounts), and providing evidence.

39. Extrapolating, controls on one form of covert non-deceptive activity will increase the demand for other, unregulated, forms. For example, regulating telephone tapping but not the bugging of premises may be expected to increase the incidence of the latter, more intrusive, activity:

> "*It should also be appreciated that there is a dynamic to the protection of human rights in the area of surveillance. 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."[24]

40. Apart from the issue of the legality of the proposed surveillance, cost is a factor. Telecommunications interception is a favoured method of surveillance because it is comparatively cheap. This was confirmed by the Australian Barrett Review in 1994, which estimated from information provided by various agencies that such interception costs AUS$570 a day, compared with AUS$1,376 for video, $1,630 for listening devices, AUS$1,895 for physical surveillance, or AUS$2,772 for vehicle tracking.[25] The different surveillance techniques all have the same object, namely 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 surveillance

41. These factors indicate that an integrated approach should be adopted to the regulation of intrusion and the interception of communications. As covert methods vary in their degree of intrusiveness, such an approach could stipulate that a more intrusive method only be resorted to when a less intrusive one is not practicable. For example, techniques which involve the physical intrusion into premises (e.g. to plant a recording device) may be more intrusive than electronic surveillance conducted by remote means. An integrated approach would have the added advantage of reducing the definitional problems arising from attempting to regulate only some surveillance activities.

42. A set of principles addressing the various calibrations of intrusion was formulated by the Canadian Royal Commission on the secret services:

"(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."[26]

Privacy and customer relations

---

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

25 *Privacy Law and Policy Reporter,* November 1994, at 1.

26 *Freedom and Security Under the Law,* Ottawa, 1981, at para 411.

43. An integrated approach would nonetheless have to accommodate the special considerations arising from the use of surveillance in connection with the provision of customer services, such as telecommunications. Service carriers will be aware that surveillance activities may adversely affect customer relations. This emerges from the recent revelation that Hong Kong Internet users' customer information was inadequately safeguarded. Supernet' s Project Manager acknowledged that the lapse could be damaging to his customers.[27] H. Jeff Smith describes an increasing consumer backlash against corporations perceived as violating privacy.[28] While consumers have tended to be largely unaware of defective privacy practices, this is changing with increasing media attention devoted to the issue. Privacy is being increasingly used as a competitive weapon as it becomes of more vital concern for consumers. The government mandated surveillance of commercially provided services generates consumer issues that do not arise outside the provision of such services.

The privacy debate in Hong Kong

44. A number of reports have been released in the last 5 years focusing in telephone tapping in the territory. In 1991 Justice released a report seeking the introduction of legislation requiring phone taps to be justified to an independent body. In March 1991 the Bar Association prepared a submission to the Human Rights Committee on the 3rd 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" and that 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."*[29]

45. On 5 April 1991, the same paper reported that the Human Rights Committee had questioned government representatives on the issue and called for additional legal protections.

46. On 26 May 1992 the *South China Morning Post* reported that the Convenor of the Omelco Constitutional Development Panel, Mr Andrew Wong, had said that the reference in section 33 of the Telecommunication Ordinance (Cap 106) to tapping in the "public interest" required explication.

47. At its meeting on 20 January 1993, the members of the Legislative Council Panel on Constitutional Development suggested that the Law Reform Commission should be requested to make a preliminary report on section 33 of the Telecommunications Ordinance. More recently, the Review Committee of the Independent Commission Against Corruption recommended a review of existing powers to intercept communications.

---

27 *South China Morning Post,* 30 January 1995.

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

29 Para. 7.4.21.

48. The most recent development was a proposed private member's bill to impose a court warrant system to regulate the interception of telecommunications and mail.[30]

Local attitudes

49. The variability of privacy attitudes between countries, and even 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. None of these questions referred to privacy as such. The questions and response are set out below, with the commonest response in bold lettering:

> *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%.
>
> *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%.
>
> *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%.
>
> *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%.
>
> *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. %;** EW:12.9%.
>
> *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%.

---

30 *South China Morning Post* 6 August 1995.

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%.

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%.

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%.

Q. *Is it necessary this should be controlled by law?*

A. **Yes: 67.9%;** No: 26.2%; Don' t know: 6.0%.

It will be observed that in response to all these questions over 50% thought that legal regulation was called for.

The sub-committee' s approach

A broad approach to protection from surveillance

50. We have conceived our initial task to be the articulation of a general, underlying, right to protection against intrusion. Only once we have defined the scope of the right of protection against intrusion can the scope of legal controls be examined. Surveillance involves the capture of personal information. An additional dimension is involved, however, namely the *intrusive* nature of the process aimed at obtaining information. The use of a surveillance device directed at your home is objectionable whether or not personal information is obtained as a result. However, we have not found it easy to define this additional dimension of concern. Wacks refers to it as "seclusion or solitude"[31], but insofar as this conveys the element of territorial privacy, it does not clearly encompass intrusive methods by remote means.

51. The individual' s *reasonable* expectation of protection from surveillance cannot be based on purely empirical considerations. A society may be rife with intrusions, but this should not preclude an individual from expecting minimum standards. *Klass*[32] and

---

31 Raymond Wacks, *Personal Information, op cit,* at 248.

32 (1974) 2 EHRR 214.

Malone[33] are quite clear that the relevant standard is what an individual should be entitled to expect in a society governed by the rule of law. The alternative is not tenable, because it would mean that the rights of the individual could be diminished by their negation in practice. A similar approach is adopted with other rights, such as freedom from torture.

52. Surveillance is often described by reference to whether it is aural or visual, and whether it targets individuals within private premises or outside them. Such an approach focuses on specific instances of intrusion. In principle, we consider the distinction between aural and visual surveillance to be irrelevant. Why should it matter what perceptual sense is being employed by the snoop? Whilst telephone calls may be overheard, letters may be read and significantly communicative non-verbal behaviour monitored. Similarly irrelevant, in our opinion, is the immediacy of the data: infrared signals signify human presence as much as photographic images.

53. A person's reasonable expectation of privacy can be broadly categorised as having the following three aspects:

a) that he will not be deliberately observed or overheard, including the recording of his activities or speech (freedom from physical surveillance); 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 shall not occur.

54. Implicit in this classification is the distinction 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). These are already partly addressed by the Personal Data (Privacy) Ordinance and the anti-hacking provisions of the Telecommunication Ordinance. Physical surveillance, however, is at present totally unregulated.

General approach to criminal sanctions

55. Having briefly considered the individual's right to, and expectation of, privacy, we now address the difficult issue of what conduct of others infringing this expectation should be subject to criminal sanctions. This is distinct from the issue of whether a civil remedy should be available. Of particular relevance is the question of whether a third party who intercepts a communication between two individuals is liable to either of them for

[33] (1984) 7 EHRR 14.

breach of confidence. This question, although relevant to the protection of privacy, is outside our terms of reference. Nonetheless, an attempt has been made to explore such issues in the Annexure.

56. 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 on this 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* : Where social need is made out, imposing criminal sanctions usefully establishes social norms proscribing clearly unacceptable conduct.

c) *Deterrence and retribution*: Establishing a criminal offence would also create a deterrent. This would be so even if no prosecution were ever brought. The regulation of surveillance addresses a unique situation because the conduct in question is by definition intended to be undetectable. Conspiracy to rob is another example of conduct deemed criminal, despite the evidential difficulties. The perpetrator of surreptitious surveillance will seldom be discovered by the victim. If he is discovered, it will either be through discovery of the device or the subsequent disclosure of the information. Access rights under the data protection law may, subject to exemptions, also indicate whether data held must have been obtained surreptitiously. Under the Personal Data (Privacy) Ordinance there are no specific sanctions attaching to the disclosure of surreptitiously obtained data.

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

57. In the light of these principles we now address in the following chapters the three privacy interests identified above, namely:

a) freedom from physical surveillance;

b) freedom from interception of telecommunications;

c) freedom from surveillance of one' s data.

Chapter 1

The regulation of physical surveillance

Summary

1.1 In this chapter we examine the regulation of surveillance of the individual. The discussion is in two parts: "territorial intrusion" and "extra-territorial intrusion."

1.2 The first of these is concerned with surveillance involving intrusion into private premises. This has two forms:

- *it may involve an intruder entering private premises. We reject making mere trespass an offence, but conclude that it should be an offence to enter as a trespasser with the intention of interfering with the privacy of the occupants*

- *it may involve what is commonly called the "bugging" of premises i.e. the placement and use of a surveillance device therein, whether it be a camera, microphone, or similar. We consider that this ongoing source of intrusion also merits criminal sanctions.*

1.3 The feasibility of regulating "extra-territorial intrusion" or surveillance at large (i.e. conducted outside private premises) is considered. We conclude that criminal sanctions should only attach to surveillance conducted outside private premises when:

- *it utilises technical devices, and*

- *it targets individuals within private premises.*

We consider these two limitations both correspond to the reasonable expectations of the individual and provide the certainty of scope necessary in criminal provisions.

Recommendations

1.4 We do not recommend the creation of a general crime of trespass. Instead, we recommend a regulatory framework for the control of physical surveillance comprising three criminal offences along the following lines:

- *entering private premises as a trespasser with intent to observe, overhear or obtain personal information thereby;*

- *placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier.*

- *placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant without the consent of the lawful occupier.*

"Private premises" in this context means any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. In addition it should cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated; school premises; and commercial premises, aircraft, vessels and vehicles from which the public are excluded.

1 TERRITORIAL INTRUSION

Introduction

1.5 Article 17 of the ICCPR (reproduced as article 14 of the Hong Kong Bill of Rights) provides in part that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, *home*, or correspondence." It adds: "Everyone has the right to the protection of the law against such interference or attacks". The European Court of Human Rights has held that an unlawful search of a person's home may constitute an interference with this right.[1]

Non-common law jurisdictions

1.6 A number of non-common law jurisdictions have legislative provisions specifically protecting the territorial privacy of *domestic* premises. Criminal sanctions are prescribed. The provisions are distinct from and additional to any provisions prohibiting surveillance by remote means. Accordingly, article 72 of the Danish constitution provides that "the dwelling shall be inviolable". The Iceland, Luxembourg and German constitutions have virtually identical provisions. Article 102 of the Norwegian constitution provides that "search of private homes shall not be made except in criminal cases". Similarly, article 172 of the Netherlands constitution protects physical privacy by allowing the entry of a dwelling without the occupant's consent only "in the cases determined by law, by virtue of a special or general order given by an order designated by law".

---

1 *X v UK* (Application No. 6184/73).

Hong Kong and other common law jurisdictions

1.7 It has been pointed out that:

> *"The common law is pre-eminently a law of property. In so far as human rights such as political participation, freedom of expression, or privacy received any protection at all, it was as an adjunct to property interests."*[2]

1.8 *Entick v Carrington*[3] provides a landmark endorsement of the rights of the individual to be protected from ministerially authorised searches on grounds of "state necessity". Nonetheless the decision is tied to property rights:

> *"The court expressly refuted the idea that a minister had the authority to issue general warrants to search for papers relating to seditious writing. Neither the argument of state necessity nor the alleged long practice behind the issue of such warrants could make up for the absence of an express statutory power of search. However, ... the decision is critically dependent upon the fact of trespass to land. It did not protect privacy as such, but property rights. The seizure of material critical of the King and his favourites occurred in the plaintiff's house, enabling him to invoke the tort of trespass."*[4]

1.9 Two legal principles deriving from property law which afford some protection from privacy intrusions are those of trespass to land and nuisance. These will now be examined.

Trespass to land

1.10 The Lord Chancellor's 1993 Consultation Paper described this remedy as follows:

> *"A plaintiff will have a civil cause of action for trespass to land when, without lawful justification, the defendant enters on the plaintiff's land, or when he remains on it after his right of entry has come to an end, or when he places or projects any object onto it. ... The plaintiff does not have to show that he has suffered any damage as a result of the trespass in order to bring the action."*[5]

---

2 Lustgarten and Leigh, *op cit*, at 41.

3 (1765) 19 How St. Tr. 1030.

4 Lustgarten and Leigh, *op cit*, at 42.

5 Lord Chancellor's Department & the Scottish Office, *Infringement of Privacy : Consultation Paper* (1993), at 56.

1.11 Trespass to land therefore involves the intrusion onto private property without lawful justification or consent. Such consent may be implied. For example, in the absence of signs to the contrary, there would be an implied consent to enter land to knock at the door. Trespass has a long history in English law and in addition to trespass to land there is trespass to goods and to the person. The fact that, unlike the latter, trespass to land was not criminal could be attributable to the complexities of the law relating to title. The tort is of limited practical benefit, due to the expense of litigation and the often paltry damages available. However, exemplary damages may be awarded "where there is an oppressive, arbitrary or unconstitutional trespass by a government official or where the defendant cynically disregards the rights of the plaintiff in the land with the object of making a gain by his unlawful conduct".[6]

1.12 In *Baron Bernstein of Leigh v Skyviews and General Ltd*[7] the plaintiff's land was flown over and an aerial photograph of his house taken without his knowledge or consent. His claim for trespass was rejected on the basis that the rights of the owner in the air space above his land only extended to such height as is necessary for the ordinary use and enjoyment of his land and the structures upon it.

Nuisance

1.13 Unlike trespass to land, nuisance is usually a continuous wrong arising out of a state of affairs, rather than a single act. The Younger Committee summarised this cause of action as follows:

> *"an action for private nuisance is normally brought for <u>some physical invasion of the plaintiff's land by some deleterious subject matter</u> - such as noise, smell, water or electricity - in circumstances which would not normally amount to trespass to land. It is much more doubtful if it would cover an activity which had no physical effects on the plaintiff's land, although it detracts from the plaintiff's enjoyment of that land. Thus spying on one's neighbour is probably not in itself a private nuisance although watching and besetting a man's house with a view to compelling him to pursue (or not to pursue) a particular course of conduct has been said to be nuisance at common law. With regard to the latter type of conduct, however, it must be admitted that it is concerned with a situation very different from the typical case in which complaint is made of an invasion of privacy. The eavesdropper or spy does not seek to change the behaviour of his victim; on the contrary he hopes that it will continue unchanged, so that he may have the opportunity of noting it unobserved."*[8]

1.14 The gist of the action in nuisance is therefore that the defendant's act disturbs the plaintiff in the enjoyment of his land. In a decision described as coming close to

---

6 Halsbury's Laws of England (4th ed), vol. 45, para 1403.

7 [1978] QB 479. See R Wacks, "*No Castles in the Air"* (1977) 93 LQR 491.

8 Younger Report, *op cit,* Appendix I, para 18.

the creation of a new tort of harassment, the Court of Appeal has recently held that the remedy may avail the victim of pestering phone calls. In *Khorasandjian v Bush*[9] the plaintiff sought relief in respect of the pestering behaviour of a jilted suitor. The court held that the persistent making of annoying and unwanted phone calls, even apart from any objectionable content, constituted a private nuisance.

1.15 In *Hubbard v Pitt*[10] it was held that besetting premises can amount to an actionable nuisance. In *Bernstein*, the court commented that no court would regard the taking of a single photograph as an actionable nuisance:

> *"But if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance from which they would give relief."*[11]

1.16 ***Requirement of proprietary interest*** As remedies for invasions of privacy, both private nuisance and trespass were until recently thought to share the same limitation that they can only be brought by the person who is the lawful "occupier" of the land affected by the nuisance or trespass. This would preclude redress by victims lacking a freehold or leasehold proprietary interest, such as patients in hospitals, guests in hotels, or even the harassed spouse or offspring of the occupier of a private dwelling. As regards the last category at least, *Khorasandjian* has held that, in view of changing social conditions, relief in nuisance should be available against annoying phone calls, regardless of whether or not there is a proprietary interest. In so doing, it adopted the approach followed in the Canadian decision of *Motherwell v Motherwell*[12] which held that a remedy in nuisance availed a spouse because "she has a status, a right to live there with her husband and children". It is not clear whether this approach would also apply to licence holders such as hospital patients or hotel guests. *Khorasandjian* does not address the issue of whether a remedy for trespass should similarly extend to occupants without a proprietary interest.

Eavesdropping

1.17 The common law offence of eavesdropping applies to listening just outside a house with the object of spreading of mischievous tales. Unlike the position in England, this offence has not been abolished by statute in Hong Kong.

Legislative developments in the United Kingdom

1.18 The common law property rights reviewed above of trespass and nuisance afford only the scantiest protection of territorial privacy. Following an incident in 1982 when

---

9 [1993] 1 QB 727.
10 [1976] 1 QB 142.
11 [1978] QB 479 at 489.
12 (1976) 73 DLR (3d) 62.

an intruder entered Buckingham Palace, consideration was given to the creation of a general offence, but no legislative proposals to this effect resulted. The United Kingdom Interception of Communications Act does not regulate the interception of conversations through the use of secret listening devices (i.e. "bugging"). 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." Hence in *R v Khan*[13] the Court of Appeal proceeded on the basis that the legislation was not applicable when considering the admissibility of evidence obtained by bugging private premises. The Court noted that the 1984 Home Office Guidelines on covert listening devices and visual surveillance (private places) did apply, but that these were not publicly promulgated. The Court commented:

> *"Although not a legal rule: 'An Englishman's home is his castle' is a tenet jealously held and widely respected. It is in our view, at least worthy of consideration as to whether the circumstances in which bugging a private home by the police could be justified should be the subject of statutory control."*[14]

1.19 Earlier, in its 1981 report, the Royal Commission on Criminal Procedure had recommended that the use of surveillance devices (including the interception of letters and telephone communications) by the police should be regulated by statute:

> *"As with all features of police investigative procedures, the value of prescribing them in statutory form is that it brings clarity and precision to the rules; they are open to public scrutiny and to the potential of Parliamentary review. ... There is the further consideration that ... the United Kingdom is required by Article 8 of the [European Convention] to bring these matters under statutory control."*[15]

1.20 Recent United Kingdom legislation does regulate surveillance generally, although only when engaged in by the secret service. The Security Services Act 1989 and the Intelligence Services Act 1994 both recognise the constitutional significance of interference with property by secret police. As trespass is not an offence under the general law, the legislation does not criminalise such activities when performed by the secret service. Instead, the approach adopted is that intrusion is expressly sanctioned when carried out pursuant to a warrant. Thus section 3 of the Security Service Act provides that "no entry on or interference with property shall be unlawful if it is authorised by a warrant". Section 5 of the 1994 Act is wider and provides that a warrant can authorise any of the three secret services (MI5, MI6, and Government Communications Headquarters) to interfere with property, trespass on land or interfere with wireless transmissions.

Law reform proposals in the United Kingdom

---

13 [1994] 3 WLR 899.

14 *Ibid,* at 910.

15 Cmnd 8092, at para 3.56.

1.21 The most comprehensive review of controls on surveillance was conducted by the Younger Committee. Its proposals are examined later in this chapter. More recently, the Calcutt Committee[16] was asked, *inter alia*, "to consider what measures (whether legislative or otherwise) are needed to give further protection to individual privacy from the activities of the press". The Committee recommended that it should be made a criminal offence to engage in any of the following intrusive activities with intent to obtain personal information with a view to its publication and without the consent of either the lawful occupant (in (a) or (b)) or the individual (for (c)):

a) entering private property; or

b) placing a surveillance device on private property; or

c) taking a photograph, or recording the voice, of an individual who is on private property with intent that the individual shall be identifiable.

1.22 In his subsequent report in 1993, Sir David Calcutt commented:

> "*The Privacy Committee made it clear that these offences should be brought into force immediately, and were not offered as an alternative to any revised form of self regulation. Many of those who submitted evidence to me, but who expressed doubts about the wisdom of introducing a statutory regime of regulation or a new statutory tort of infringement of privacy, were nevertheless of the view that physical intrusion should be outlawed. On 14 December 1992 the Independent and on 16 December 1992 the Daily Telegraph both supported the introduction of criminal offences. I remain of the view that the criminal offences should be enacted. The offences do not attempt to cover every wrong associated with physical intrusion. But they do cover the most blatant forms of physical intrusion and, if enacted, would make clear forms of conduct which were wholly unacceptable."*[17]

1.23 Calcutt's recommendations were directed to the press. This is entirely attributable to the fact that the committee's terms of reference were restricted in those terms. There is nothing in either the report of the Calcutt Committee or Sir David Calcutt's subsequent report to suggest intrusions were more acceptable when pursued for other purposes. As mentioned above, even intrusions for the purposes of state security are now dealt with by statute.

---

16 *Report of the Committee on Privacy and Related Matters* (Calcutt Committee), 1990, Cmnd 1102.

17 David Calcutt , *Review of Press Self-Regulation*, 1993, Cm 2135, para 7.4.

1.24 The subsequent National Heritage Committee Report (1993) commented that the Government "welcomed the proposed criminal offences in principle", but that the Home Office had subsequently "identified several [unspecified] difficulties".[18]

1.25 The United Kingdom Government released its White Paper *Privacy and Media Intrusion: The Government's Response* in July 1995. It concludes that:

> *"The Government has long recognised that there is, in principle, a case for the introduction of offences. ... [but] has, however, so far been unable to construct legislation which, in practice, would be sufficiently workable to be responsibly brought to the statute book."*[19]

1.26 Specific points made in the White Paper which are relevant to the Calcutt proposals referred to above, or to proposals made by ourselves, include:

- The difficulty in drawing the line between public and private property. We do not accept this as a sufficient reason for not attempting to do so.
- A defence of occupier's consent "would allow occupiers to connive in physical intrusion of others on their own property". We address this later.
- The need to define "surveillance device". Our recommendations recognise this and we refer to a "sense-enhancing, transmitting or recording device."

1.27 A number of commentators have noted that the United Kingdom Government faced political difficulties if it enacted offences specifically targeting the Press.[20] Yet that was the quandary created by narrow terms of reference focusing solely on the activities of the media. Our own terms of reference are cast in general terms, facilitating a more thorough examination of the arguments of principle, such as how to define the human right encompassed in the term "privacy" and the extent to which it should be protected.

Territorial privacy and criminal sanctions

1.28 Two approaches are possible in imposing criminal sanctions to protect territorial privacy: making simple trespass a crime or making trespass a crime if accompanied by intent to conduct surveillance. This section also examines a complementary offence of placing surveillance devices on private premises without consent.

(1) Simple trespass

1.29 In English law there is no general criminal offence of trespass to land. It is, however, an element of such offences as burglary. One approach, therefore, would be to

---

18 National Heritage Committee, *Privacy and Media Intrusion: Fourth Report*, 1993, Vol. I, para 23.

19 Cm 2918, paras 3.3 and 3.4.

20 Barendt E, *Britain rejects media privacy law* (1995) 2 PLPR 109.

make trespass a criminal offence. This would only be merited, we believe, in respect of intrusion into a private *dwelling* rather than land generally. A dwelling may be a house, room, tent, or caravan. This focus on protection against physical intrusion into domestic premises would accord with the European provisions cited above. Whilst caution should be exercised in plucking out a provision from differing legal systems, a number of local ordinances utilise the notion of a dwelling when defining powers of entry by agencies such as the Urban Services Department. The underpinning provided by article 14 of the Hong Kong Bill of Rights is also relevant, with its reference to protection of the "home". Implementation of that provision does not, however, require the creation of criminal sanctions.

1.30 A general crime of trespass along these lines would not merely protect property interests but would also recognise a distinct privacy interest, namely that of territorial privacy. The required criminal intent would be that of intrusion into the territorial space of the dwelling. Nonetheless, we feel some disquiet about a general crime of trespass. We are concerned that one undesirable consequence would be to criminalise comparatively innocent trespasses. This would be particularly likely as the intruder's motives are irrelevant in trespass: "The requisite intent is present if the defendant desires to make an entry, although unaware that he is thereby interfering with another's rights." Creating a general offence along these lines is outside our terms of reference. Such a proposal may also impact on existing laws and practices, such as police powers. Our other major concern is the lack of a demonstrated need for such an offence. As mentioned above, a tort action already provides a civil remedy. Forcible entry would also be caught by the offence of criminal damage.

1.31 **For these reasons, we decline to endorse the creation of a general crime of trespass.**

(2) Trespass with intent

1.32 A stronger argument can be mounted for the creation of an offence of entry to private premises *with intent* to conduct surveillance. A crime in these terms would include the simple activity of surveillance, whether or not a device was used. Such an offence could be similar to that proposed by the Calcutt Committee set out above. Examples of laws which provide for an offence of trespass with intent to engage in surveillance can be found in the United States in the state legislation of Maine and Utah. In the former state, a person is guilty of an offence if he "commits a civil trespass on property with the intent to overhear or observe any person in a private place." In Utah, the equivalent provision refers to a person who "trespasses on property with intent to subject anyone to eavesdropping or other surveillance in a private place." Proof of the necessary intent would be a question of fact in each case.

1.33 Unlike the Calcutt recommendation, these formulations specifically refer to trespass. An advantage of so doing is that the concept of trespass with intent is well understood and regularly applied by lawyers.

1.34 We recommend below an offence of placement of a surveillance device in private property. A supplementary provision extending to surveillance activities, along the lines of the US provisions to which we have referred, accords with an integrated regulatory approach addressing all options. This reduces the prospect of an unregulated gap being utilised by those anxious to avoid criminal penalties. **We accordingly recommend that it should be an offence for a person to enter private premises as a trespasser with intent to observe, overhear or obtain personal information therein.**

1.35 This formulation's reference to overhearing or observing would provide clear protection from intrusion and would safeguard seclusion. This is distinct from in principle, but may overlap in practice, the obtaining of personal information. The difficulty is that entry to private premises will inevitably result in the acquisition of private information. Effectively, then, including this ingredient could arguably criminalise any trespass - a result contrary to our earlier decision. In practice it will not because of the requirement of proving this specific intent beyond reasonable doubt. For example, the evident intention of a burglar caught with a bag of jewellery is to steal, not to obtain personal information.

1.36 ***"Consent"*** The question of *whose* consent is required also needs to be addressed. The Calcutt Committee recommends that the consent required be that of the "lawful occupant". We agree with this, but there are difficulties. In premises such as hotels and hospitals, the legal owner will not be the victim of the intrusion, but rather the licensee. Similarly, in the case of rented premises it will be the tenant. **We recommend that the law be so framed that legal protection is extended to potential victims of intrusion such as guests in hotels and tenants in rented premises.**

(3) Physical intrusion by means of technical devices

1.37 The placement of hidden surveillance devices on private premises (known as "bugging") constitutes a continuing intrusion on private premises. A remedy, albeit mild, is already available in civil trespass upon the discovery of a bugging device, *provided* the culprit can be found. The advantage of making such conduct a criminal offence is that assistance can be provided in identifying the source of the bug. We also think that the bugging of premises is a sufficiently serious intrusion into the individual's privacy to warrant criminal deterrence. **Accordingly we recommend that it should be an offence for a person to place, use or service in, or remove from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier.**

1.38 This formulation basically accords with the Calcutt recommendation dealing with this aspect. However, servicing or removal are also caught, as they are under the Canadian provision. But we prefer Calcutt's reference to "placement" rather than "installation" as it better accommodates the planting of mobile devices. Calcutt's reference to "with intent to obtain personal information" we discard as inappropriate. We recognise that specifying the occupier's consent would sanction the eavesdropping of visitors to domestic dwellings.

1.39 In view of this recommendation dealing with surveillance by technical means, we have reviewed the need for the offence recommended earlier of entering private premises as a trespasser with the intention of obtaining personal information. It is not an ingredient of that offence that technical devices are used. We consider such a provision a necessary supplement to the anti-bugging offence, to avoid a gap sanctioning surveillance within private premises by human instead of technical means. It would also catch the snooper interrupted before he can place a device.

1.40 ***"Private premises"*** An offence of intrusion into private premises with intent necessitates a definition of "private premises". The Calcutt Committee adopted the following:

> "*any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. In addition it should cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated."*[21]

1.41 In his subsequent report, Sir David Calcutt proposed that the definition be extended to include school premises.

1.42 We prefer a definition along the lines of Calcutt, but extending beyond domestic premises to commercial premises, aircraft, vessels and vehicles to which the public are excluded. **We accordingly recommend that for the purposes of the two offences proposed above prohibiting trespass with intent to obtain personal information and bugging of premises, "private premises" means any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. In addition it should cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated; school premises; and commercial premises, aircraft, vessels and vehicles from which the public are excluded.**

2 EXTRA-TERRITORIAL INTRUSION

Introduction

1.43 Having examined the regulation of intrusion into private premises, we now consider the regulation of surveillance at large.

1.44 The individual may reasonably expect the protection of his privacy from any activities of snoops or spies. In principle, the reasonable expectations test should not be

---

[21] Calcutt, *op cit,* at paragraph 6.34.

restricted to protection from the use of high-tech devices, but should include such covert low-tech activities as peeping through a key hole. It would also encompass overt deception. For example, the undercover agent would, in a sense, be observing the individual with the subject' s knowledge. Nonetheless, an element of deception is involved. As such, the agent would be performing a similar function to the plant of a secret device.

1.45 The individual' s expectation of privacy is not therefore be related exclusively to the use of devices. Our researches indicate, however, that elsewhere both laws and recommendations for reform addressing surveillance at large (that is, conducted other than from within private premises) have a narrower focus than that of protection from intrusive activities generally. Reference to devices is usually included in the formulation of a criminal offence of physical surveillance. All the laws reviewed in the Younger Report do so. Similarly, the recommendations of the Younger Committee, the English Law Commission, and the Australian Law Reform Commission all incorporate reference to devices.

A reasonable expectation of privacy[22]: The Younger Committee

1.46 The most comprehensive recent attempt to develop a general test for regulating privacy was that of the Younger Committee. It proposed a criminal offence of surreptitious surveillance by means of a technical device. The offence would involve:

(a) A technical device providing electronic and optical extensions of the human senses. All devices are covered, whether or not they are designed with the main purpose of surreptitious surveillance. The necessary intent (see (b)) relates to the use to which the device is put and not its design. Ordinary household devices such as binoculars are accordingly encompassed along with sophisticated spy gadgets.

(b) Surreptitious use of the device. The Younger Committee considered that surreptitious surveillance is qualitatively different from other objectionable forms of surveillance. It recommends that both be regulated, but only the former should be dealt with by criminal sanctions. "Surveillance" as used by the Younger Report also includes the interception of communications, including telecommunications. We separately address the interception of telecommunications later in this paper.

(c) A person who is, or whose possessions (such as documents, databases, etc.) are, the subject of surveillance. That is to say, regulation extends beyond that of the issue being currently examined, namely physical surveillance, to surveillance of data. In 1972 when the Younger Committee reported, "hacking" was not a problem. It has since been recognised as a phenomenon accorded separate protection.

---

22 *Katz v United States* 389 US 347 (1967).

(d) A set of circumstances in which, *were it not for the use of the device*, that person would be justified in believing that he had protected himself or his possessions from surveillance whether by overhearing or observation. This provides a reasonable expectations test. By virtue of the italicised words, it does not require the individual to take precautions against the sense-enhancing devices involved, but only against surveillance by unaided senses. The blinds need not be drawn, regardless of what one is doing, if the nearest apartment is some distance away.

(e) An intention by the user to render those circumstances ineffective as protection against overhearing or observation.

(f) Absence of consent by the victim. The notion of consent to *surreptitious* surveillance is paradoxical and the Committee states that it would be "rare, but it is theoretically conceivable."

1.47 Why this restricted focus on surveillance by *devices* by the Younger Committee and by laws regulating surveillance at large? Such a limitation ignores intrusive activities not deploying technical devices. The point is not explicitly addressed by the Younger Committee's report. Rather, the report's approach appears to reflect the concerns of the many organisations who submitted evidence to that Committee. It would appear the community's concerns about surveillance relate primarily to technical surveillance. These no doubt relate to the individual's greater vulnerability to being surreptitiously observed when this is done by means of technical devices. This is discussed in the next paragraph.

1.48 Related to the fact that social concern about surveillance appears to be most acute in relation to technical surveillance, there are policy reasons for limiting prohibition of surveillance to surveillance carried out using technical devices. The individual's expectations of privacy outside his home must be balanced by considerations of what conduct by others it is reasonable and feasible to regulate. In this context, the reference to devices in the Younger Committee's proposed offence is supported by the following considerations:

(a) **Lack of self-protection**: The difference between physical surveillance conducted at large by means of technical devices on the one hand and by unaided senses on the other is that in the former case the individual is unable to take effective measures to protect himself from intrusion. Normal physical barriers that can be relied on to prevent penetration by unaided senses are ineffectual in the face of technical devices. Accordingly, the need for legal regulation is greater.

(b) **Avoiding regulation of everyday activities**: An additional argument against extending the regulation of physical surveillance to unaided observation relates to the nature of the conduct to be proscribed. Casual observation of others in public places is a normal feature of everyday life. Some forms of unaided observation may not be casual, such as peering

through a high window on a ladder. We are not satisfied that such conduct is a problem which merits making it a criminal offence. Legislative overreach will vitiate the perceived legitimacy of the law. The common law protections already available, such as eavesdropping and private nuisance, are reviewed above. The arcane nature of that jurisprudence reinforces the suspicion that the activity is not a significant problem. This is not the position with the proliferation of surveillance devices. This is viewed as a new social phenomenon meriting legal intervention in the same manner as computerisation provided the impetus for data protection laws.

(c) **Technical problems**: The technical objections to the legal regulation of non-casual unaided surveillance are also formidable. We would anticipate drafting difficulties involved in framing a prohibition. The necessary intent would be that of surveillance. Where devices are not deployed, problems of proof are likely to be acute. Reference to devices would facilitate proof. Even so, we recognise that few convictions are secured, for example, under Telecommunication Ordinance provisions relating to the use of radio apparatus. Whilst the issue of principle should be kept distinct from that of detectability, this can only be pursued up to a point.

Conclusion on use of devices

1.49 In view of the above we conclude that an offence of surveillance at large should be restricted to surveillance involving the deployment of technical devices. The proposed offence is defined later in this chapter.

Distinctions between devices

1.50 The Younger Committee recommended the regulation of "devices" defined as "electronic and optical extensions of the human senses". It added that this definition "should be wide enough to cover any likely developments in the foreseeable future". It is of course important not to couch provisions susceptible to technological change and this definition arguably achieves this. The report clearly envisaged that "devices" encompassed recording devices.

1.51 In its recommendations extending the duty of confidence, the Law Commission in England adopts a slightly different approach and distinguishes between "a device made or adapted solely or primarily for the purpose of surreptitious surveillance" and "any other device (excluding spectacles and hearing aids) which are capable of being so used". The Commission explains:

> *"Examples of devices falling within the second category are ordinary binoculars and an ordinary tape recorder which may be used to record the conversation of participants at a meeting, either openly or secretly by hiding it under the table. There may be situations when surveillance devices of the latter kind are used to which those subject to that*

surveillance should not reasonably take exception, if they are or ought reasonably to be aware of it and they could without undue inconvenience take precautions to avoid the surveillance in question."[23]

1.52 We propose adopting in this context also the definition used in the anti-bugging provision set out above, namely "sense-enhancing, transmitting or recording device". This makes it clear that the perceptual sense involved is irrelevant. This broad coverage avoids the gaps which have occurred in other jurisdictions. For example, the Australian Privacy Commissioner has recently noted that in that country whilst the federal law prohibits interception of communications and state laws prohibit listening devices to overhear private conversations, intrusive video surveillance has been left unchecked.[24]

Is an offence of surveillance by device sufficiently precise?

1.53 The remaining issue is whether such a restriction is not only necessary but also sufficient in framing an effective criminal sanction. The requirement that usage of the device be *surreptitious* would provide a limitation. By this we do not mean that the device be specifically concealed but simply not reasonably visible to the victim e.g. a camera mounted on a distant building. It was noted that the *surreptitious* use of a sense-enhancing device was an element of Younger's proposed offence. As the Younger test itself recognises, however, surreptitiousness cannot be a *sufficient* element of such an offence. Also relevant is the expectation of privacy/implied consent to observation of those subject to surveillance. For example, an individual may be readily observable by others generally (e.g. on a street) but is observed by binoculars some distance away. Should this be prohibited? We think not, and agree with the Australian Law Reform Commission that:

"It is not desirable, nor would it be feasible, to regulate the use of surveillance or recordings in ... entirely public places. People who are in a public place must anticipate that they may be seen, and perhaps recorded, and must modify their behaviour accordingly."[25]

1.54 This is not to say that expectations of privacy may never be infringed by overt surveillance, although the reasonableness of the expectation would be affected by social definitions, such as, for instance, a social consensus that security requirements justified video cameras in banks. Also, public surveillance raises additional issues of its own:

"For example, it seems reasonable to think that, from an individual viewpoint, surveillance in public is less damaging than intrusion into private places, especially if it is announced and unavoidable. However, whilst this may well be true when considering whether to target a particular person, the analysis cannot stop there. It must also take account of the chilling effect such surveillance - even, and

---

23 Law Commission, *Breach of Confidence* (Law Com No 110), 1981, Cmnd 8388, para 6.37.

24 *Proceedings of the Joint Australian/OECD Conference on the Global Information Infrastructure*, 7-8 February 1996, Canberra.

25 Australian Law Reform Commission report on *Privacy* (1986), at paragraph 186.

perhaps especially, if publicly announced - will have on others. This can be seen most clearly in relation to participation in demonstrations, signing petitions, or any other form of political activity which enables the participant to be identified individually."[26]

1.55 Generally speaking, however, we agree that the individual's expectation of privacy in public premises must acknowledge not only the risk of being observed, but of those observations being recorded. We doubt the feasibility of recognising the legitimacy of unaided observation of a passer-by, yet prohibiting the use of a concealed camera by that same passer-by. We agree with the Younger Committee that people must expect to be photographed in public and that a ban would not be sustainable.

1.56 For these reasons, the regulation of surveillance by means of remote devices, whether or not surreptitiously used, requires additional restrictions. The two main options are:

a) adoption of the complex additional requirements of the Younger test limitations, or;

b) excluding from regulation surveillance of persons not in private premises, along the lines of Calcutt and various laws.

The Younger test

1.57 Younger proceeds on the basis that the privacy of any situation is relative and cannot be dealt with by a simple dichotomy between whether it occurs in private or public premises. Instead of a restriction cast in terms of property, the Younger Committee's formulation of the offence of surreptitious use of such devices contains the following ingredients:

"a person who is the object of surveillance;

a set of circumstances in which, were it not for the use of the device, that person would be justified in believing that he had protected himself or his possessions from surveillance whether by overhearing or observation;

an intention by the user to render those circumstances ineffective as protection against overhearing or observation; and

absence of consent by the victim."[27]

---

[26] Lustgarten and Leigh, *op cit,* at 47-48.

[27] Younger Report, *op cit*, para 563.

1.58 According to this test it would be an offence to subject an individual to surveillance by means of technical devices wherever he/she was located, provided the victim reasonably believed there was protection from surveillance. The additional elements combine to screen out situations such as the street observation described, but they also make for a degree of complexity that we consider undesirable or even unworkable in a criminal provision. This difficulty is compounded by the imprecise and hypothetical "were it not for" test. This would appear to be the price entailed by a flexible test encompassing surveillance of persons on public premises, but nonetheless one screening out surveillance of those agreeable to being observed (whether or not surreptitiously).

1.59 The Younger test was not followed by Calcutt, nor does it appear to be embodied in any legislative provision of which we are aware. Calcutt comments that the recommendation has not been implemented "mainly because of the difficulty in defining the act which it is intended to prohibit".

1.60 We accept that Younger's "reasonable expectation" test of privacy against remote surveillance is the ideal solution. We have concluded, however, that this test is unsuitable for inclusion in the criminal law. From a technical viewpoint, it is insufficiently precise to constitute a criminal standard. Even where a reform is accepted as socially desirable, drafting difficulties may prove insurmountable. Also, from a policy viewpoint, we think it too wide. It would accord protection (and hence criminal liability) in situations lacking demonstrable social need. Hong Kong's highly urbanised environment apparently engenders relative acceptance of the privacy risks involved. Finally, we doubt if the broader test has any prospect of generating the political support necessary for it to become law.

Restricting offence to surveillance of private premises

1.61 The alternative is to restrict the regulation of devices by reference to the nature of the premises subject to surveillance. The basis of this approach is that people can be presumed to expect privacy when not on public premises and, conversely, those disposed to conduct surveillance can be presumed to be aware of this. The principal advantage of restricting the offence of remote surveillance to private, or at least non-public, premises over the Younger test is simplicity: it avoids the application of a "reasonable expectations" test that may be thought insufficiently precise for inclusion in a criminal provision.

1.62 Nor do we think that the Younger test's focus on reasonable expectations is necessarily inconsistent with the ostensibly narrower one excluding surveillance in public places: Hong Kong conditions are unlikely to generate a reasonable expectation of privacy in its public places. To incorporate a reference to premises in the test is effectively to recast the reasonable expectations test in more definite terms. We accept, however, that the application of such a restriction may exclude some cases. Ideally, we would wish to cover all individuals where they have a reasonable expectation of privacy. However, we do not consider it feasible to cast criminal provisions in sufficiently broad terms to achieve this. For example, we recommend below that it be a defence to the offence of surveillance within

private premises that consent be provided by a lawful occupier, notwithstanding that this may countenance a host bugging his guest.

Conclusion on additional restriction on scope of surveillance at large

1.63 In view of the above we conclude that an offence for surveillance at large should, in addition to being restricted to surveillance involving the deployment of technical devices, be restricted by reference to the nature of the target premises.

1.64 Two variants of a restriction in terms of target premises are possible:

a) only regulating technical surveillance targeting private premises; or

b) regulating all technical surveillance *except* in relation to public premises.

1.65 The first approach was adopted by Sir David Calcutt in his 1993 report following up on that of the Privacy Committee.[28] He noted that the anti-bugging offence proposed by the Privacy Committee required a surveillance device to be "placed" on private property. However, this ignored the capacity of surveillance devices to be used effectively at considerable distances. He therefore accepted the need for a supplementary provision of using a surveillance device (whether on private property or elsewhere) in relation to an individual who is on private property, without the consent of that person.

1.66 This approach is also adopted by a number of laws. For example, the Utah law provides that it is an offence if a person intentionally:

> *"installs or uses outside of a private place any device for hearing, recording, amplifying, or broadcasting sounds originating in the place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy there."*

1.67 It will be observed that neither this formulation nor Calcutt's includes as an element of the offence that usage be surreptitious: it is sufficient that it is without consent. While the Younger Committee thought surreptitiousness a key concern, we consider it less germane to a recommendation prohibiting surveillance of private premises. We consider that remote surveillance is objectionable whether or not it is conducted surreptitiously: awareness that one's home is the target of laser sensors across the way should not constitute a defence.

1.68 The alternative formulation of this approach is to frame the offence in terms that surveillance by means of devices in respect of non-public premises should be an offence. We note that "public place" is defined by section 3 of the Interpretation and General Clauses Ordinance (Cap. 1) as follows:

---

[28] David Calcutt , *op cit.*

"'Public place' means-

(a) any public street or pier, or any public garden; and

(b) any theatre, place of public entertainment of any kind, or other place of general resort, admission to which is obtained by payment or to which the public have or are permitted to have access."

1.69 We have carefully considered an exclusion of "public places" instead of specifying "private property" as the target premises requiring protection. This alternative, negative, test of *excluding* public premises recognises that the real test is not ownership but the right to control access to the site. This would mean, for example, that protection would extend to hotel rooms but not the lobby. The difficulty is that "public premises" will be open at certain times but closed at others. We have concluded that it would be difficult to have a moving target. In particular, it would complicate consideration of the issue as to whose consent is required: the occupier or, when open, the visitors.

1.70 **We therefore recommend that it should be an offence for a person to place or use a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring without the consent of the lawful occupier either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant. We further recommend that the definition of "private premises" proposed above in relation to entering as a trespasser with intent, or the bugging of premises, should be adopted for the purposes of this offence.**

Scope of offence

1.71 The question of overlap with the hacking offence under the Telecommunication Ordinance arises. We recognise that surveillance of an individual's activities and his data are conceptually distinct. However, one view is that surveillance of data represents an intrusion not dissimilar from observing one's physical activities. While our core concern is physical surveillance, it is increasingly difficult to distinguish this from surveillance of data. Hence our concern to protect people from intrusion in the broadest sense. Whether the offences dealing with physical surveillance and data surveillance are drafted separately is a technical matter. One concern is that if they are separated, some matters may fall between the cracks.

1.72 The main difficulty with drafting the offences separately would be one of proof. It would be a defence to raise a reasonable doubt as to whether the defendant was conducting surveillance of persons, or of data, on the private premises in question. It should be noted that the offence is not constituted by the installation of a surveillance device, but requires an intent that the device is to be used for monitoring. This would exclude accidental surveillance or hacking. This will be a question of fact and there will be situations where the surveillance device can be shown to be targeting particular premises.

1.73 A consequence of the adoption of this requirement that the device must be installed or operated *outside* the premises in question is that such complex issues as the legitimacy of workplace and shop surveillance are not addressed thereby.

Chapter 2

Interception of communications: technical aspects

Summary

2.1 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 intercepts can be effected 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.

2.2 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

2.3 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 represented by the presence or*

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

2.4 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]

2.5 Just as computers have become increasingly efficient, so have modems, with affordable models transmitting bits per second, 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]

2.6 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*

---

1 Fitzgerald and Leopold, *Stranger on the Line: The Secret History of Phone Tapping* (1987), at 222-226.

2 *Ibid.*

3 *The Economist,* 16 October 1993.

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

and telephones has become blurred. The 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 to the phone, such as "call forwarding". 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 (such as the case where calls to a Florida probation service were re-routed without warning to a New York pornographic phone hotline). 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 Brian Clough and Paul 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]

2.7 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 discernible changes to the telephone circuit being tapped."*[6]

2.8 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 order of magnitude 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

2.9 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. Locally, Hong Kong' s 190,000 mobile phone users are particularly vulnerable. As an article in the International Herald Tribune put it, calls can

---

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

6 *Ibid,* at 228.

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]

2.10 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.

2.11 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 algorithym and a high speed array processor computer is required to crack the code. However, recent reports have stated that digital systems have been successfully hacked into.

2.12 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

2.13 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 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*

---

7 *International Herald Tribune,* 23 June 1992.

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

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 a target line, caused by the current flowing through it, which can be analysed to reveal the traffic on the line."[9]

Analysis of transmissions

2.14 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]

2.15 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 conversation, regardless of who says it. Complex mechanisms accommodate the fact that speech is continuous and speech signals do not generally abide by well defined boundaries.
- 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. Such a system could, for example, be used to trawl out all international calls made from any telephone by a particular political activist. "[11]

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

---

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

"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 being 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."[12]

Message systems of telecommunications systems

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

Facsimile

2.18 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.[13] 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

2.19 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's computer screen. E-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 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."[14]

---

12 *Ibid,* at 31.

13 Quoted in S*outh China Morning Post* 20 February 1990.

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

2.20 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. 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."*[15]

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

2.22 A technical aspect of E-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."*[16]

2.23 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 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."*

---

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

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

Hong Kong's telecommunication system

2.24 In July 1994 Hong Kong hived off supervision of telecommunications from the Post Office to a newly created Telecommunications Authority. Ben A Petrazzini of the Hong Kong University of Science and Technology explains:

> *"The new regulatory body, which shares organisational features with the British Oftel (i.e. small body headed by a director with considerable regulatory power), is in charge of licensing, financial monitoring and regulation, management and administration of frequency spectrum, the development of technical standards and equipment testing. The general policy guidelines for the sector will remain the domain of the Economic Services Branch (ESB).*
>
> *In early 1994 the ESB produced a position paper that summarised the recent reforms and those being considered for implementation in the near future. Without any doubt, one of the most important and bold reform steps is the forthcoming liberalisation of local basic services. This decision upsets the conventional sequence of liberalisation (i. e. ; first, international services, and later, only in very selected cases, competition in the local market), turning Hong Kong into the first territory in the world to reverse the order of reform adopted elsewhere.*
>
> *This counterintuitive move was inspired by a timing difference in licensing agreements. While the international basic services license (held by Hong Kong Telecom International) runs until 2006, the license for basic local services (held by the Hong Kong Telephone Company-HKTC) expires on June 30 1995. The initial decision to open the local loop to competition was taken in May 1992. Three new operators were selected: Hutchison, New T&T Hong Kong, and New World Telephone."*[17]

2.25 The *Far East Economic Review* provides the following statistics: Hong Kong's telecommunications market is worth $36 billion. It has a per-capita traffic rate five times higher than the United States and 20 times higher than Japan. It has four competing cellular companies and 34 paging companies. Its per capita subscription rate of one pager for every six people is the world's highest. It is the world's largest single market for the CT2 system (which enables a person to call out, but not to receive calls: 95% of CT2 buyers use pagers).[18]

Eavesdropping in Hong Kong

---

17 *Transnational Data and Communications Report,* July 1994, at 35.

18 *Far East Economic Review,* 3 February 1994.

2.26 As mentioned above, the government does not presently provide figures on the number of taps 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.

Chapter 3

Statutory regulation of communications

Summary

3.1 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.*
- *Section 27A prohibits unauthorized access to any program or data held in a computer.*

3.2 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 Hong Kong Bill of Rights will be discussed in the next chapter.

3.3 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. Section 13 covers not only mail carried by the Post Office, but also e-mail and that carried by private courier services. The powers in section 13 are broader than those of its counterpart in the Telecommunication Ordinance.

1 REGULATION OF TELECOMMUNICATIONS

Offences under the Telecommunication Ordinance

Interference with telecommunications equipment

3.4 The Telecommunication Ordinance 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."*

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

3.5 This obscure 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 apt to cover the interception of *telecommunications*, as opposed to telecommunications equipment. This is also the case with regulation 9(1) of the Telecommunication (Control of Interference) Regulations 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 working of the apparatus, so as to avoid detection.

Licensing of scanners and receivers

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

> *"(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].”

3.7 As at 30 August 1992, no licences had been issued, according to a *South China Morning Post* report. The *SCMP* reported 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.” Portable handheld radio scanners can be easily concealed in a coat pocket. Police have reportedly discovered transreceivers tuned to police radio bands in the course of raids.[1] The concern that criminals were able to monitor police movements prompted the Telecommunications Authority in 1994 to increase financial penalties ten fold (to $50,000) under the Telecommunication Ordinance. A prison term of up to 2 years remains prescribed. 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.[2]

3.8 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.

3.9 Also, of marginal relevance is the United Kingdom Wireless Telegraphy Act 1949 which has been applied to Hong Kong by the Wireless Telegraphy (Colonial Ships and Aircraft) Order, 1954 (S. I. No 488). However, the Order only applies to British ships and aircraft registered in British dependent territories. The provisions with privacy implications are identified by the Younger Report. Under section 1(1) it is an offence to install or use any apparatus for wireless telegraphy except under licence. Section 19(1) defines “wireless telegraphy” in a way that excludes devices using wires. Section 5(b)(i) prohibits the unauthorised use of wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of any message. Younger comments that this provision applies to a message:

> *“whether sent by means of wireless telegraphy or not, as it is technically possible to pick up telephone conversations by wireless telegraphy apparatus. This provision seems specifically designed to protect the privacy of ‘messages’ and that expression is not limited.”*[3]

Hacking

3.10 “Hacking” is the unauthorised accessing of a computer program. 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

---

1 *Hong Kong Standard,* 8 October 1993.

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

3 *Younger Report,* at 300.

transmitted by the phone network. The receiving computer's modem converts the signals back into computer commands. Hacking has very definite 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 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.*"[4]

3.11 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.*[5]

3.12 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.

3.13 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.[6]

3.14 With the digitalisation (and hence computerisation) of Hong Kong's telephone system, hacking also now constitutes a commonly employed technique for effecting the interception of communications. The details are explained above in the discussion of telecommunications privacy.

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

---

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

5 *Ibid,* at 64.

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

"(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. "

3.16 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."

3.17 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 dubbed as the "buster bunny" was convicted of hacking into the databases of two Hong Kong educational institutions.

3.18 In the 1980 decision of *R v McLaughlin*[7], 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 defendant was a student who made use of the university computer by gaining access from one of 300 remote terminals. 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."[8]

3.19 Press reports indicate that a similar 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.[9]

3.20 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

---

7 (1980) 53 CCC (2D) 417.

8 *Ibid, at 425.*

9 *South China Morning Post,* 27 March 1992.

in any computer". In *Attorney-General's Reference (No. 1 of 1991)*[10] the defendant had keyed commands into a computer and thereby obtained by means of *the same computer* a discount. At first instance the court held that a second computer had to be involved. Upon appeal by the Crown, counsel for the defendant argued in support that the offence is aimed at hacking, a term not used in the Act, and that "hacking" means using one computer to access another. Applying the ordinary principles of statutory interpretation, the Court of Appeal rejected this argument and held that "any computer" should not be interpreted as meaning "any *other* computer". The Court also found "persuasive" the Crown's argument that to hold that the offence required access by another computer would create " a surprising, and indeed unlikely, lacunae":

> *"[Counsel for the Crown] pointed out that there would be nothing in the [Computer Misuse Act 1990] to meet what is itself a mischief frequently encountered today, namely industrial espionage or obtaining information as to security details or other confidential information which may be stored on a company's computer ... [so that] going straight to the in-house computer and extracting confidential information from it could be committed with impunity."*[11]

Personal Data (Privacy) Ordinance

3.21 While anti-hacking provisions target the intruder, the Personal Data (Privacy) Ordinance 1995 imposes requirements on data users reasonably to safeguard the storage and transmission of *personal* data. Principle 4 of the Ordinance provides:

> *"Security of personal data*
>
> *All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to*
>
> *(a) the kind of data and the harm that could result if any of those things should occur;*
>
> *(b) the physical location where the data are stored;*
>
> *(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;*

[10] [1992] 3 All ER 897.

[11] At 438.

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data"

3.22 "Data user" in this context may, under the definition in section 2(1), be the person storing or transmitting the data. Section 2(12) is also relevant in this context. This provides:

> *"A person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes."*

3.23 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 are lax in protecting their confidential data. They observed a common misconception that computer risks were limited to breakdowns and viruses.

Authorising intercepts to telecommunications: section 33

3.24 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 authorizsed 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."*

3.25 We examine in the next chapter the human rights jurisprudence on interception of communications. Suffice to say at this stage that section 33 in does not explicitly address the various matters requiring attention if the Hong Kong Bill of Rights Ordinance is to be complied with.

3.26 The operation of section 33 was the subject of a Legislative Council question on 11 November 1992. 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?"

3.27 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."

3.28 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 10 additional staff to enable it to increase its tapping capability from 50 to 80 lines.[12]

2 REGULATION OF MAIL: THE POST OFFICE ORDINANCE

3.29 In addition to telecommunications, controls on postal communications are directly relevant to our reference. The regulation of postal service provided by the Post Office is addressed by the Post Office Ordinance (Cap. 98). That Ordinance contains considerably more elaborate provision 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

[12] *South China Morning Post,* 9 July 1995

"includ[ing] everything which is transmissible by post." The Ordinance defines a number of offences safeguarding mail delivery. These are accompanied by very wide powers of interception.

Offences under the Post Office Ordinance

3.30 The Ordinance prohibits:

- the wilful opening of any postal packet addressed to some other person (section 27).
- To fraudulently retain, wilfully secrete, keep or detain any postal packet or any mail bag (section 28).
- Without lawful authority or excuse to open, take out contents, have in his possession, or delay any postal packet or mail bag (section 29).
- Destroy any mail bag or postal packet (section 26).
- sending by post "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" (section 32)

3.31 These offences are accompanied by extremely wide powers of interception. Furthermore, whilst warrants are provided for, these are not required "if the Postmaster General has reason to believe that any postal packet has been posted . in contravention of this Ordinance" (see section 12). Given the broad provisions of section 32 quoted above, this requirement will be readily satisfied.

Authorising intercepts to mail

3.32 The provision addressing warrants is section 13 and is wide:

> *"Warrant of Chief Secretary for opening and delaying postal packets*
>
> *(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 necessary for the purpose of obtaining a warrant under this section."*

3.33 It will be observed that this is even broader than its counterpart, section 33 of the Telecommunication Ordinance. Section 13 lacks any reference to a "public interest" requirement, and the authorising officer is the Chief Secretary rather than the Governor.

3.34 It follows that the Post Office Ordinance purports to sanction the interception of mail for whatever reason. Its likely incompatibility with article 14 of the Hong Kong Bill of Rights Ordinance will become more apparent with Chapter 4's discussion of the *Klass* and *Malone* cases.

Chapter 4

The legal protection of privacy of communications

Summary

4.1 This chapter examines the common law and human rights protections for communications. It will be seen that the common law provides no effective protections 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 two reasons. Firstly, 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. Secondly, the provisions of article 17 are replicated in article 14 of the Hong Kong Bill of Rights. That provision provides statutory protection against interference by the public sector in Hong Kong. We conclude that the present provisions of the Telecommunication Ordinance and Post Office Ordinance do not accord with the requirements discussed in this chapter.

The common law protection of privacy of communications

Malone v Metropolitan Police Commissioner (No. 2)[1]

4.2 The Chancery Division decision of *Malone* comprehensively reviews the common law position regarding telephone tapping. The matter was subsequently taken to the European Court of Human Rights (see below) and the court's ruling provided the impetus for the United Kingdom Interception of Communications Act. The decision accordingly continues to describe the United Kingdom legal position for tapping not covered by the Act. Although the application of the Hong Kong Bill of Rights Ordinance substantially affects the position in Hong Kong, the common law position remains relevant as it may buttress protections under the Bill of Rights.

4.3 Malone was a British citizen arrested in 1977 and charged with handling stolen goods. The jury was unable to reach a verdict at both the trial and a subsequent retrial and the case was dropped. However, during the first trial cross-examination of a police officer resulted in a surprise admission that Malone's phone had been tapped.

[1] [1979] Ch 344.

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.

4.4 Malone adduced the following arguments:

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.

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. That offence had, however, been repealed by the Criminal Law Act 1967 (but it has not been repealed in Hong Kong). But even apart from this, the judge thought that telephone tapping was outside the mischief of the doctrine. American jurisprudence was considered of little avail and this submission, too, was rejected.

Confidentiality The court held that there were three conditions to the application of this principle:

- 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.

4.5 Applying the principle, the Court held:

"*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."[2]
"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 . . . the 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."[3]

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

4.7 In its report *Breach of Confidence,* the English Law Commission referred to this finding, 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."[4] Their recommendation that the duty of confidence be extended to apply to surreptitiously obtained information is examined in the Annexure.

4.8 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."[5]

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

European Court decisions on interception of communications

4.10 Article 14 of the Hong Kong Bill of Rights provides in part that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". That provision is in identical terms to article 17 of the International Covenant on Civil and Political Rights ("ICCPR"). Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms ("the European Convention") provides that "everyone has the right to respect for his private and family life, his home and his correspondence". Article 8(2) states that "there shall be no interference

---

2 *Ibid,* at 360.
3 *Ibid,* at 376.
4 Law Commission Report No 110, at para 6.35.
5 Schwarz L B, *"On Current Proposals to Legalise Wiretapping"* (1954) 103 *Univ. of Pa. Law Rev.* 157, 162, quoted in Wacks, *op cit,* at 247.

by a public authority" with the exercise of the right under article 8(1) "except such as is in accordance with the law ...". In view of the lack of relevant jurisprudence under the ICCPR, it is necessary to look for assistance in interpreting article 14 of the Hong Kong Bill of Rights to the decisions of the European Court of Human Rights which interpret the similar provisions of article 8 of the European Convention.

4.11 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* and *Malone*. 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.

Klass v Federal Republic of Germany[6]

4.12 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. 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.

4.13 It is worth commenting on the finding that it is the possibility rather than the demonstrated fact of surveillance that is relevant. This recognises that an important feature of surveillance is its very imperceptibility. As David Lyon comments:

> *"... undetected surveillance keeps those watched subordinate by means of uncertainty. You simply comply, because you never know when 'they' might be watching. Information technology enables surveillance to be carried out in ways even less visible than those available in Orwell's, let alone Kafka's, days."*[7]

---

6 (1978) 2 EHRR 214.

7 David Lyon, *The Electronic Eye: The Rise of Surveillance Society,* (1994), at 60.

4.14 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 Professor Wacks' position (quoted above) that the essential objection to surveillance is independent of the quality of information thereby obtained: it is that there has been an intentional interference with the individual's interest in seclusion or solitude.

4.15 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.'*[8]

4.16 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.

[8] (1978) 2 EHRR 214, paras 49 and 50.

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 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.

4.17 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.

4.18 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 guarantees 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[9]

4.19 This is the most recent case in which the European Court has considered the adequacy of a law sanctioning the interception of telecommunications. It 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.

4.20 The statutory provisions governing the matter were general in nature, conferring an investigative judge with a discretion to authorise any "investigative measure" he deems necessary or useful. There must be a grounds 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.

4.21 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/offences susceptible to interception warrants
- the duration of interception warrants
- the specification of procedures regarding summarisation of intercepted conversations
- the erasure or destruction of the tapes

4.22 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."

4.23 We note that the provisions of neither the Telecommunication Ordinance nor the Post Office Ordinance address any of the matters which the European Court held in *Huvig* required addressing.

Malone v United Kingdom[10]

---

9 (1990) 12 EHRR 528.

10 (1984) 7 EHRR 14.

4.24 *Malone* is the genesis of the United Kingdom Interception of Communications Act. 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 of Human rights.

4.25 ***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.

4.26 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 one 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."*[11]

4.27 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.

4.28 The Court then turned to consider whether the interferences were justified as "in accordance with law" under article 8. "In accordance with 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:

---

[11] (1984) 7 EHRR 14, para 64.

> "*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 dangerous interference with the right to respect for private life and correspondence ... 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.*"[12]

4.29 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.

4.30 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. Application procedures were detailed in a circular to police. On issue of the warrant, the interception was effected by the telecommunications authority by 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

[12] (1984) 7 EHRR 14, paras 67 and 68.

purposes of investigation, and then destroyed. The information was used solely for investigative purposes and is not tendered in evidence, nor disclosed to others. The individual whose communications have been intercepted is not informed of the fact, even when the surveillance and the related investigation has been terminated.

4.31 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 . . . [in] the opinion of the Court, 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."*[13]

4.32 The Court accordingly concluded that the minimum degree of legal protection to which citizens are entitled under the rule of law was lacking.

4.33 ***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 such a 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. The practice had been made public in answer to parliamentary questions.

4.34 The Court noted that the metering process makes use only of signals sent to itself as the provider of the telephone service for the legitimate purposes of billing and the

---

[13] (1984) 7 EHRR 14, para 79.

investigation of complaints. No monitoring or interception of the contents of telephone calls is 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.

4.35 The remaining issue was whether such interference was "in accordance with 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).

4.36 We recommend in chapter 6 that a warrant be required to authorise any interceptions of communications falling within the scope of the proposed offences prohibiting such activities. As the release of metering data by the telecommunications authority to the police does not in itself involve any interception of communications, the police do not need a warrant before they could gain access to such data. However, insofar as the metering data relate directly or indirectly to an individual, the collection and use of such data are subject to the provisions of the Personal Data (Privacy) Ordinance.

4.37 ***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 legislation[14]. It noted that "for many years a carefully controlled system of ministerially authorised interceptions has existed". It pointed out that this was acknowledged in the *Malone* decision, but that the Court concluded that the law did not indicate with reasonable clarity the scope and manner of exercise of the discretion conferred on public authorities. The Government therefore proposed 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)*. 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 Telecommunication Ordinance or the Post Office Ordinance in Hong Kong.

Implications for the Telecommunication Ordinance and Post Office Ordinance

---

[14] *The Interception of Communication in the United Kingdom*, Cmnd 9438, 1985.

4.38 It will be recalled that section 33 of the Telecommunication Ordinance provides that the Governor or an authorised officer may order the interception or detention of communications "whenever he considers that the public interest so requires". Section 13 of the Post Office Ordinance goes even further and omits even a general public interest test. Accordingly, neither Ordinance can be said in the language of *Malone* 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. Accordingly in the remainder of this paper we examine proposals which will satisfy the requirements spelt out in the jurisprudence examined above.

Chapter 5

Interception of communications: legal issues

Summary

5.1 In this chapter, we endeavour to identify the mischief to be addressed in regulating the interception of communications. We conclude that controls are required for both the "interception" and "interference" of communications during the course of their transmission. Nor should these controls be restricted to communications transmitted by telecommunications systems. We think that face-to-face communications also merit protection.

Recommendations

5.2 Communications should be safeguarded from interception or interference (including destruction or diversion) in the course of their transmission. It should be an offence:

- *intentionally to intercept or interfere with (whether or not by means of a technical device) a communication transmitted by a distance communications system. Distance communications systems would encompass not only telecommunications system but also manual systems such as mail*

- *intentionally to intercept or interfere with a "communication" by means of a technical device (whether or not the communication itself is mediated by means of a technical device), provided that the interception could not have been effected without the use of a device.*

"Interference" for the purposes of these offences should include destruction or diversion.

Preliminary issues

"Interception" of "communications"

5.3 At the outset, it is necessary to identify the mischief to be regulated, and whether this is aptly expressed by the terms "interception" or "interference" of communications.

"Interception"

5.4 The United Kingdom, United States and Australian Acts focus on "interception." "Interception" is not defined in the United Kingdom Interception of Communications Act 1985. Halsbury states that:

> *"it is thought that it has here its ordinary meaning, i.e. 'to seize, catch or carry off on the way from one place to another' (Shorter Oxford English Dictionary) or 'to stop and seize in passage' (Chambers Twentieth Century Dictionary)".*[1]

5.5 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."*[2]

5.6 The Canadian Criminal Code provides that "intercept" means "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof."[3]

Interception in the course of transmission

5.7 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 moment, it leaves the possession of the proposed sender, or after, or at the moment, it comes into possession of the intended receiver." In other words, implicit in the concept of "intercept" is that it must occur in the course of transmission. Both the United Kingdom and Australian legislation are explicit about restricting their focus in this manner. Section 6(1) of the Australian Telecommunications (Interception) Act 1979 provides:

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

5.8 Similarly, the United Kingdom Act restricts the offence to "intentionally intercept[ing] a communication *in the course of its transmission*."[4] Unlike the United States and Australian formulations which focus on *telecommunications* purposes, the United Kingdom Act also extends to postal mail.

---

1 Halsbury's Statutes, Vol 45, at 417.

2 Omnibus Crime Control and Safe Streets Act of 1968, Title II I ("Wiretap Act"), section 2510.

3 Criminal Code (RSC 1970, c. C-34, as amended), Part IV. I, section 178.1.

4 Interception of Communications Act 1985, section 1.

5.9 We agree with this express focus on interception in the course of transmission, rather than extending the offence(s) to cover unauthorised access following transmission. We believe that it is necessary to clearly delineate the types of interception or access which merit additional controls on the basis of the gravity of their intrusiveness. In our view, interference in the course of transmission, and the immediacy of intrusion in these circumstances, falls into this category. Even so, 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 for an occupier to open a letter addressed to another person at that address would constitute interception, notwithstanding the fact that the formal delivery had been completed. 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 and no interference need result. An analogous situation would be where someone browses over faxes that have piled up in the addressee' s absence.

"Interference"

5.10 We note that "interference" rather than "interception" of correspondence is protected under the privacy provision of the ICCPR, reproduced in article 14 of the Bill of Rights. In a United States decision "interfere" was defined (not with reference to the ICCPR) 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."*[5]

5.11 In some respects, "interference" has a wider ambit than the above 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 corruption or diversion of the communication, without necessarily becoming acquainted with its contents.

5.12 Whilst we wish to restrict the focus to protection during the course of transmission, we are concerned to regulate the corruption of the communication occurring during its transmission. We have reached the conclusion that the terms "intercept" and "interfere" taken singly may not suffice. **We therefore recommend that**

---

[5] *People ex re. Benefit Ass' n of Railway Employees v. Miner* 387 Ill. 393, 56 N. E. 2d 353,356

communications should be safeguarded from interception or interference (including destruction or diversion) in the course of their transmission.

"Communication"

5.13 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." 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.

5.14 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.

5.15 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.

"Correspondence"

5.16 We note that "correspondence" rather than "communication" is protected under the privacy provision of the ICCPR and reproduced in article 14 of the Bill of Rights. "Correspondence" would appear narrower than "communication" in that it connotes distance communication whereas "communications" also encompasses that occurring face to face. On this basis, notwithstanding their differences, both telecommunications and mail can be described as involving "correspondence." Both are also likely to involve a service provider, but whereas interception of telecommunications will usually involve technical devices, this may not be the case with the interception of mail.

5.17 There are a number of reasons to legally protect correspondence from interception or interference in the course of transmission:

- it is a requirement of the ICCPR and the Hong Kong Bill of Rights Ordinance

- it accords with the reasonable expectations of both parties to the correspondence

- insofar as correspondence utilises a service provider, interference by a third party also affects the service provider.

- 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. Also relevant are the concerns of the global marketplace: the need for security of communications in such areas as banking and theft of proprietary information are two such concerns. Security is the "key component for the continued success of the information highway". Failure to afford legal protection to privacy and security of communications will ultimately slow the development of advanced networks.

5.18 We accordingly recommend that it should be a criminal offence intentionally to intercept or interfere with correspondence (eg a communication transmitted by a distance communications system) while it is in the course of transmission. This would encompass both mail systems and communications conducted by means of telecommunications systems (eg e-mail). This would include PBX systems (private telecommunications systems), which nonetheless involve service carriers. These systems are utilised by employers and other closed user groups, in conjunction with service carriers.

"Telecommunications systems"

5.19 The exchange of "correspondence" will generally be provided by telecommunications systems. In other jurisdictions controls are framed in terms specifically focusing on the interception of "telecommunications systems". For instance, section 7(1) of the Australian Telecommunications (Interception) Act 1979 provides:

> *"A person shall not-*
>
> *(a) intercept;*
>
> *(b) authorise, suffer or permit another person to intercept; or*
>
> *(c) do any act or thing that will enable him or another person to intercept,*
>
> *a communication passing over a telecommunications system. [our underlining]"*

5.20 "Telecommunication system" is defined as meaning a system controlled by the Australian Telecommunications Commission in connection with the provision of a telecommunication service.

5.21 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*". The Act is accordingly broader than the Australian Act because it encompasses both postal and telecommunications systems. Regarding the latter, the ambit of the words quoted was considered in *R v Effik*[6]. 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.

5.22 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 (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.

5.23 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. For the appellants, it was urged that it was artificial to separate the transmission of signals through the public and then private system, as without the prior transmission through the former they would never have been received at their destination. A suggestion that the legislature would not have countenanced, for instance, a journalist intercepting calls by attaching a listening device to a privately owned handset, was countered by the argument that the legislature was unlikely to have intended criminalising "an anxious parent eavesdropping on a teenage child's conversation with an undesirable acquaintance by listening on an extension telephone."

5.24 The Court concluded that the interception did not fall within section 1 because the policy of the Act was:

---

[6] [1994] 3 WLR 583

> "*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.*"[7]

5.25 In the result, it was held that the Act did not prohibit the interception and the evidence was therefore not excluded. The appeals against conviction were accordingly dismissed. In accordance with the principle that under English law everything is permitted which is not prohibited, the interception was legal.

5.26 Even before *Effik* it was clear that the Act did not apply to eavesdropping not involving 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." Halsbury, however, comments that there is nothing expressly excluding these forms of surveillance from the ambit of the legislation, but in *R v Khan*[8] the Court of Appeal proceeded on the basis 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.

5.27 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.*"[9]

5.28 This is presumably a reference to the ability of an individual using a private system to avail himself of such privacy technologies as cryptography (the use of encryption). These technologies are dealt with in Chapter 9, but it is worth reiterating 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. British Telecom's monopoly as a service provider was abolished by legislation in 1981 and licences were granted to Mercury Communications and other service providers. In 1984 BT was privatised and half its interests sold to private investors. Nonetheless, official links

---

7 [1994] 3 WLR 583, at 592.
8 [1994] 3 WLR 899
9 [1994] 3 WLR 583, at 592.

are retained: under the Telecommunications Act the Secretary of State may issue BT with directives in the interest of national security and these would extend to telephone tapping.

5.29 It follows that the United Kingdom Act' s distinction between "public" and "private" systems hinges on whether or not the system is licensed. We consider that such questions raise public policy and economic issues which would be more appropriately pursued elsewhere as a separate exercise. Our earlier recommendation that interception of "correspondence" be made a criminal offence encompasses both public and private systems. We note that *Malone* makes no distinction between public and private telephone systems.

5.30 The United States has gone in the opposite direction to the United Kingdom and has not restricted the scope of its legislative control to public telecommunications systems. In October 1994 Congress approved legislation revoking a provision which excluded cordless telephones from protection under the wiretapping law. "Thus in the future, intercepting a cordless conversation, even the radio portion between the handset and the base unit, will require a warrant."[10]

5.31 Similarly, the current controls in Hong Kong do not focus on public telecommunications systems. Whereas section 27 of the Telecommunication Ordinance provides that it is an offence to damage, remove or interfere with a telecommunication installation with intent to " prevent or obstruct the transmission or delivery of a message; or intercept or discover the contents of a message", section 33 is broader and provides:

> *"Whenever he considers that the public interest so requires, the Governor, or any public officer authorised 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 in the order."*

5.32 "Telecommunication" is defined in section 2 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."*

5.33 It will be observed that there is no reference to telecommunications systems and arguably the provision (which empowers, not prohibits) extends to auditory surveillance as well.

---

[10] *Privacy Journal,* October 1994

Focus on telecommunications systems inadequate

5.34 Having recommended above protection from interference or interception of communications transmitted by distance communications systems, we have considered whether such a provision is sufficient. Insofar as the protection recommended above is restricted to communications transmitted by distance communications systems, we think it should be supplemented. In our view, the protection of telecommunications systems raises *additional* public interest concerns supplementing the privacy interests as such. These concern the protection of the integrity of the *systems* themselves, quite apart from the protection of specific communications transmitted by such systems. Regarding the latter, there is an argument that there are interests *additional* to the protection of the reasonable expectation of privacy. These are well stated by the President of the United States Telephone Association who comments that if the public becomes skittish 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. This also implies an additional factor distinguishing the interception of communications *networks* from one on one personal surveillance: namely, that with the former there is a third party involved. Furthermore, that third party is in a contractual relationship with the communicant.

5.35 Our recommendations on the protection of correspondence should address these concerns. This is because distance communications will encompass communications networks supplied by service carriers. However, we consider Hong Kong should not follow the United Kingdom in *restricting* the focus on the integrity of telecommunications systems. Such an approach is too narrow by denying protection to communications intended to be private which are outside such systems. Our core concern is with the protection of privacy interests as such. We note that under article 14 of the Bill of Rights, protection is afforded not only to correspondence, but to "privacy". Doswald-Beck has commented that "the term 'private life' [in article 8 of the European Convention] is meant to have a meaning of its own, independent of rights relating to family, home and correspondence".[11] In both *Klass* and *Malone* the European Court held that telephone conversations are covered by *both* the notions of correspondence *and* private life.

5.36 The protection of face to face communications accordingly merits consideration. Such communications will not constitute "correspondence". To some extent, however, such communications will be covered by our recommendations on surveillance. It will be recalled that surveillance comprises observation (visual or auditory) of a person's behaviour/activities (including speech) by means of technical devices when the observed person is in private premises. We recommended above that surveillance should be prohibited by the following offences:

> *a) placing or use of a surveillance device outside private premises with the intention of obtaining personal information therein without the consent of the lawful occupier.*

---

[11] Doswald-Beck L, The Meaning of the 'Right to Respect for Private Life' under the ECHR, (1983) 4 HRLJ 283.

b) placing, using, servicing on, or removing from, private premises a surveillance device without the consent of the lawful occupier.

c) entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein.

5.37 These offences are intended to regulate the intrusive process whereby the individual's ongoing behaviour is observed and/or recorded. Such conduct is objectionable, regardless of whether personal data is collected as a result: the concern with intrusion is distinct from and additional to concerns as to the collection and use of personal data, hence the need for protections supplementing the Personal Data (Privacy) Ordinance 1995. The references at (a) and (c) above to "obtaining personal information" would cover observation of the individual's personal environment (such as, for instance, the type of books or videos kept by the individual). It is therefore wider than observing or recording an individual's behaviour as such.

5.38 The restriction of the application of these offences to private premises is thought to correspond to the reasonable expectation of freedom from observation. Accordingly, these proposed offences would cover behaviour (including speech) conducted within private premises. It follows that where one party is communicating from public premises, only one half of the conversation would be caught by our proposal. This is unsatisfactory, because a communication between two parties is considered to be greater than the two parts. Indeed, they may not apply at all because both the parties to the communication may be in public premises. The territorial restriction is not relevant to the protection of private communications. Accordingly the comprehensive protection of private communications requires supplementary provisions which omit reference to a territorial test. However, for consideration is what alternative restrictions may be necessary to accord with a reasonable expectation test. It will be recalled that the purpose of restricting our general surveillance recommendations by reference to both technical devices *and* their application to private premises is to make the proposed offences sufficiently certain in their application.

5.39 The issue accordingly arises whether we should supplement our proposed prohibition on interference with distance communications systems by specifically regulating the interception of communications. There appear to be at least three, partially overlapping, situations:

a) the simple interception of communications, including the overhearing of conversations, whether or not the conversation and/or interception is mediated by technical means

b) the technically-aided interception of communications, whether or not the communication itself is mediated by technical means;

c) the interception of distance communications systems involving a network/service carrier

5.40 Point (c) is already specifically addressed by our recommended offence. Points (a) and (b), however, encompass face to face oral communication, whether conducted in public or private premises. Only by discarding the territorial restriction of our surveillance recommendations will the anomalies referred to above be removed. The most fundamental issue is whether there is sufficient pressing need to attach criminal sanctions to the interception of *conversations* conducted outside private premises. Even to the extent there may be such an expectation in some circumstances, should that expectation be protected by the criminal law? The majority of members believe that they should.

5.41 A minority viewpoint is that criminal sanctions should not be extended even to technically-aided interceptions of conversations conducted in public. It was argued that this would represent an overreach of the criminal law to cover situations not meriting criminal sanctions. According to this view it is open to individuals to reduce the risks of interception by retiring to private places. However, given the capabilities of modern technology summarised in the introduction, such risks remain, and may even be enhanced because it is easier to locate a target in private premise than in a public place - hence the frequent featuring of rendezvousing spies in parks. If so, this is a less than compelling argument that there is an insufficiently pressing social need to protect communications conducted in public places.

5.42 Accordingly we consider that the protection of the criminal law should be accorded to protect private communications, provided that the offence is specific enough to address a real social need. One approach would be to prohibit the monitoring of "private communications" by means of technical devices, whether or not those communications are conducted in whole or in part on private premises. For example, the Canadian Criminal Code prohibits the interception of "private communications" by means of a surveillance device. Everyone who, without the consent of at least one of the parties to the communication, intercepts a private communication by means of a surveillance device is guilty of an offence.[12] "Intercept" is defined as including "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof."[13]

5.43 We endorse this approach, which would make it an offence to intentionally intercept a communication by means of a technical device. This would result in the protection of unaided conversations generally. On the other hand, the requirement that the interception be conducted by means of a surveillance device usefully delimits its scope by excluding the casual overhearing of conversations. This accords with the reasonable expectations test: the individual cannot reasonably expect not to be overheard by passers-by. The reference to technical devices in effect subsumes the reasonable expectation test, as the use of such devices defeats the expectation of privacy. We think that this should be assumed, whether or not the intercepted party had failed to avail himself of any readily available encryption system. While the requirement reflects the reasonable expectations test, it is more precise in its application than that test. This is an important attribute of a proposed

---

12 RSC 1985, volume III, C-46, section 184.

13 *Ibid,* section 183.

criminal offence. Prosecutions would be rare but the offence would nonetheless set appropriate norms deterring such conduct.

Consistency with previous recommendations on surveillance

5.44 It is important that our recommendations in relation to interception of communications should not conflict with those in respect of personal surveillance. The proposed offences regulating surveillance incorporate two restrictions, namely use of a device, and the application of that device to *private* premises. Does then the regulation of auditory monitoring of behaviour in public places accord with our previous recommendation excluding from regulation the visual monitoring of behaviour? In our view, there is no contradiction between retaining a territorial restriction (i.e. the monitoring of private places) in the context of the regulation of personal surveillance, and discarding such a restriction when addressing the interception of communications. In both cases, the relevant basis is the individual's reasonable expectation of privacy. Presence in a public place would usually negate any expectation to be free from observation, and our limitation on the regulation of surveillance accordingly corresponds with the reasonable expectations test. However, the reasonable expectation of privacy of communications is less readily determined by territorial considerations. Privacy of communications is a distinct, if sometimes overlapping, interest from that concerning freedom from observation. Arguably, a "communication" is greater than the sum of the input of the two communicants. Alternatively expressed, the creation of a shared communication generates an extra dimension to the observation of the "behaviour" of the participants. Personal surveillance, however, is concerned more with the monitoring of the component behaviour of the individual participants, including speech. We acknowledge that even here, the element of interaction may be significant.

5.45 In view of the matters canvassed above, **we recommend that it should be an offence:**

a) intentionally to intercept or interfere with (whether or not by means of a technical device) a communication transmitted by a distance communications system. Distance communications systems would encompass not only a telecommunications system but also manual systems such as mail

b) intentionally to intercept or interfere with a "communication" by means of a technical device (whether or not the communication itself is mediated by means of a technical device), provided that the interception could not have been effected without the use of a device.

"Interference" for the purposes of these offences should include destruction or diversion.

5.46 The non-inclusion of a "device" in (a) acknowledges the interception of manually delivered mail may not involve any technical device and, indeed, may require additional controls. Similarly, parties may correspond by, for instance, flags. In this context, we are disposed to think that the reasonable expectations test should be retained as an additional ingredient of (a). However, use of a communications system is subject to a more definite expectation of privacy than some conversations. As regards (b), as discussed above we think that the reasonable expectation test is subsumed by the requirement that it be effected by a technical device. The proviso that the communication could not have been effected without the use of such a device is added to exclude communications which could in any event be casually overheard by a third party.

5.47 As regards both offences, the necessary intent should be to intercept *any* correspondence/communication, not just a specific item. The transmission medium utilised should be irrelevant.

5.48 If our proposed offences are adopted, section 27 of the Telecommunication Ordinance can be repealed. It will be recalled that this presently constitutes the sole general prohibition of interceptions and provides that:

> *"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. "*

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

Consent

5.49 Legislation elsewhere usually provides that it is a defence that *one* of the communicants consented to the interception. Interception without a warrant is permissible where there is consent. The issue of consent does not really arise in the case of surveillance. It arises with interceptions because two parties are involved. 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. Section 2511(2)(c) of the United States Wiretap Act is similar, but requires that one of the parties has given prior consent. Actual consent is similarly a defence under the Canadian Act.

5.50 We agree to the adoption of such a defence and prefer the United Kingdom formulation, which provides that it is a defence if the interceptor believed on reasonable grounds that a communicant has consented.

5.51 PABX systems highlight the fact that taps may not just be effected by an external agent, such as a service carrier, but also by the immediate operator of the system, such as the employer. The consent issue is more ambiguous in this situation, where the carrier's sole role is to provide telecommunications services and he has no additional relationship with the communicant.

Chapter 6

The regulatory framework

Summary

6.1 Having defined the offences regulating surveillance and the interception of communications, we now consider the regulatory framework. In this chapter we examine the role of a warrant system in the authorisation of intrusions. We conclude that all surveillance and interception of communications proscribed by our proposed offences should require authorisation by warrant on public interest grounds. We define the "public interest" with some particularity. Applications for warrants should be considered by a High Court judge, to ensure that they receive independent scrutiny by an impartial authority.

6.2 We then examine restrictions on the retention of surveillance and materials obtained through interception, including the issue of whether such material should be admissible in prosecutions.

Recommendations

6.3 A warrant should be required to authorise all surveillance or interception of communications falling within the scope of the proposed offences prohibiting these activities. All applications for warrants for surveillance or interception should be made to the High Court.

6.4 The sole grounds for issuing a warrant authorising intrusions should be **either** *that it is for the purpose of preventing or detecting serious crime where:*

- *there is probable cause for suspicion of the target; and*
- *the information is not reasonably available by less intrusive means.*

or *that it is for the purpose of security, defence, or international relations in respect of Hong Kong where:*

- *the intrusion is likely to be of substantial value in furthering these purposes; and*
- *the information cannot be reasonably obtained by other means.*

"Serious crime" should mean either an offence punishable by at least 7 years imprisonment, or an offence punishable by at least 3 years imprisonment where there

"Security" should include safeguarding the stability of the local financial system.

6.5 A warrant should be issued for an initial period of 60 days and renewals should 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.

6.6 In circumstances where it is impractical 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.*

6.7 Authorisation by warrant should be available to sanction intrusions by both public authorities and private companies.

6.8 Provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985 should be adopted, including the imposition of a requirement that the warrant-issuing authority ensure that adequate steps are taken to achieve compliance with the stipulations set out at paragraph 6.57. Surveillance and intercept materials should be inadmissible as evidence, regardless of their relevance. This prohibition should extend to both authorised and unauthorised surveillance/ interception of communications. The prohibition should cover not only the fruits of surveillance but also details of methods used.

A warrant system: handling of exceptions

The need for warrants

6.9 Two main approaches are possible in determining the scope of statutory exceptions:

a) stipulating that they are defences, the applicability of which will only be authoritatively determined by a court (similar to the approach adopted under the Personal Data (Privacy) Ordinance). However, the intrusions in question here are more severe than misuse of data.

b) implementing a warrant system, requiring reasons to be stated, which is challengeable in court.

6.10 A warrant system is essential:

a) where the authority cannot effect the intrusion without technical assistance (for instance, by the telecommunication service provider) and/or;

b) where the activity in question is likely to be challenged, such as physical entry to premises.

6.11 From a strictly pragmatic perspective, a warrant system is less necessary where the intrusion can be effected surreptitiously and without outside assistance.

6.12 Under the Personal Data (Privacy) Ordinance exceptions are self-executing, but reviewable. Under this system, the exception is invoked by the data user on the basis that the terms of the statutory exemption apply, but this is subject to challenge by the data subject, and will then be reviewed by a supervisory authority. While this system should suffice in dealing with departures from the data protection principles, we consider it inadequate in sanctioning the more serious intrusions entailed by surveillance and the interception of communications. In addition, use of exemptions under the Personal Data (Privacy) Ordinance is more transparent - data subjects will become aware of refusals of access and many changes of use. By way of contrast, an individual will seldom become aware of being made the subject of surveillance or interceptions.

6.13 The alternative is a warrant system. This is the conventional mechanism adopted by, for instance, the United Kingdom legislation in sanctioning intrusion to property and interception of communications. It has two advantages. Firstly, it entails approval by an independent authority prior to the intrusion being 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 either:

a) required the technical assistance of a third party. This is the usual position when intercepting public telecommunications systems. While it is theoretically possible for a law enforcement agency to unilaterally hack into the public telecoms switching programs and effect taps, it is much simpler and surer to approach the public telecoms company and request that they arrange matters; or

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.

6.14 We note that in the United Kingdom all intrusions regulated by law (and hence the warrant requirement) fall into one or other of these categories. However, our recommendations propose much more comprehensive regulation of surveillance, whether or not interceptions or physical intrusion are involved. The issue therefore arises whether a warrant should also be required in those situations where the intrusion requires no external assistance and is inherently undetectable. Indeed, most remote surveillance falls into this category.

6.15 We have concluded that a warrant requirement should extend to this latter situation also, so that it would apply to all proscribed surveillance and interception activities. A warrant procedure is merited in view of the seriousness of all such intrusions. Furthermore, to subject only some intrusions to the warrant procedure would encourage snoops to turn to 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. **We accordingly recommend that a warrant be required to authorise all surveillance or interception of communications falling within the scope of the proposed offences prohibiting these activities.**

Who should issue warrants?

6.16 Regarding the nature of the authority to authorise the warrant, we note that in the United Kingdom this is a government Minister, 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. Section 2 of the Interception of Communications Act 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:

> *"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."*[1]

[1] Lustgarten and Leigh, *op cit,* at 55-56.

6.17 Hong Kong courts already grapple with security issues in dealing with public interest immunity certificates in criminal trials. In the United Kingdom, judges perform the roles of Commissioner for Interceptions and Commissioner for the Security Service. The issue was addressed in *US v United District Court*[2]. The United States Government submitted that the courts were not equipped to assess security matters but this was unanimously rejected by the Supreme Court:

> *"We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. ... There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. ... If the threat is too subtle or complex for our senior enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance."*[3]

6.18 We consider that the additional independence afforded by a judicial determination is necessary in Hong Kong. We note that section 44(2) of the Personal Data (Privacy) Ordinance provides that prior to obtaining the identification of journalistic sources, the Privacy Commissioner must obtain the approval of the High Court. We think that this should similarly be the case in the authorisation of warrants sanctioning intrusions, whether the public interest invoked relates to law enforcement or to security in respect of Hong Kong. It is important that friction be avoided between the judiciary and the executive. Dividing-up the issuing of warrants according to whether they relate to crime (for the judiciary) or security (for the executive) would be difficult. The advantage of having a judge scrutinise all applications is that it ensures that those applying for the warrant will have to think the matter through. This diminishes the prospect of abuse of power. It is also reassuring to the public. Restricting the power to the High Court should also make for greater consistency of approach. **Accordingly, we recommend that all applications for warrants for surveillance or interception should be made to the High Court.**

6.19 We do not think that the judge's consideration of a security-related warrant would entail his making an independent assessment of the factual issues, as suggested by the United States Supreme Court. What it would require would be that the judge be satisfied that authorisation is warranted on the basis of the broad picture deposed to by relevant officials. For example, the affidavit may state that as a result of information received, it was reasonably believed that a terrorist attack was imminent.

6.20 As with other *ex-parte* warrants, we envisage that they would usually be dealt with on paper. A hearing would seldom be required. The issue of closed hearings does not arise. The duty judge system will provide 24 hour access. Regarding emergency taps, such as in hostage or other life-threatening situations, we think that such interceptions should be subsequently ratified by judicial authorisation. We recognise the impracticability in

---

2 407 US 297.

3 *Ibid,* at 320.

such circumstances for an application to be made to a judge in every case before interceptions to be initiated, but note also that dispensing with a system of *ex post facto* authorisation could seriously undermine the safeguard of judicial scrutiny. **We therefore recommend that in circumstances where it is impractical 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.**

Private sector intrusions

6.21 In other jurisdictions the warrant system envisages the approval of intrusions by public authorities. In principle, however, in some situations private agencies may be able to make out a case why their surveillance/interception activities would further one of the public interests we have identified as justifying intrusion, such as the prevention or detection of serious crime. For example, companies that wish to avoid the embarrassment of a police investigation often hire private investigators to investigate offences. **We recommend that authorisation by warrant should be available to sanction intrusions by both public authorities and private companies**. However, private sector applicants should have to satisfy a more stringent public interest test.

United Kingdom legislative developments regulating the security services

6.22 We note that in the United Kingdom the provisions of the Interception of Communications Act has been extended to the regulation of surveillance when conducted by the secret services. The Security Service Act 1989 applies to MI5 and the Intelligence Services Act 1994 applies to MI6. The genesis of the 1989 Act was a ruling of the European Commission of Human Rights regarding complaints by office holders of the National Council for Civil Liberties (NCCL), an unincorporated association which works to monitor and defend civil and political rights in the United Kingdom. The complaints arose from allegations that the office holders had been the subject of surveillance by MI5. The allegations were made by a former MI5 officer, in a television interview in 1985 and repeated in an affidavit sworn for the purposes of a judicial review.[4] In line with government policy of not disclosing information about the operations of the Security Service, the United Kingdom neither confirmed nor denied the applicant's allegations.

6.23 The European Commission noted that although the applicants did not allege that they were specific targets of telephone or mail intercepts, their evidence was that they had been subject to "indirect interception", i.e. the recording of information about them which appeared in the telephone or mail intercepts of targets. The Commission found that there was a reasonable likelihood that the applicants were the subject of secret surveillance. It therefore had to consider whether such interference was "in accordance with the law". The Commission applied the *Malone* test cited above of a law which is sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which surveillance may apply. It noted that the Security Service exists for the exclusive purpose of the defence

[4] Application No 12175/86.

of the Realm. The Security Service's activities were governed by a Directive, but not authorised by law:

> *"Members of the Security Service are public officials but unlike, for example, police officers, immigration officers or officers of HM Customs and Excise, they have conferred on them not special powers whether under any law or by virtue of the Directive. Although the Directive is published, it is not claimed by the Government that it has the force of law or that its contents constitute legally enforceable rules concerning the operation of the Security Service. Nor does the Directive provide a framework which indicates with the requisite degree of certainty the scope and manner of the exercise of discretion by the authorities in the carrying out of secret surveillance activities."*[5]

6.24 The Commission accordingly found that there had been a violation of article 8 of the European Convention because the surveillance was carried out by a body which had no legal authority, and therefore was not authorised by law. Anticipating an adverse ruling to similar effect by the European Court, the legislation was introduced. MI6, the security service concentrating on foreign intelligence, and the Government Communications Headquarters was also now put on a statutory footing under the Intelligence Services Act 1994. That Act also establishes a system of parliamentary accountability of both these services and MI5.

6.25 Section 1 of the Security Service Act 1989 provides that the function of the Service (i.e. MI5):

> *"shall be the protection of national security and, in particular, its 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.*
>
> *(3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."*

6.26 This explication, if not an exhaustive definition, of "national security" is useful, in view of former United States Attorney General Griffen Bell's comment that "national security" has become a "talismanic phrase" which has been used "to ward off any questions about the legitimacy of any governmental conduct to which the phrase was applied."

6.27 The general structure of the legislation is similar to that of the Interception of Communications Act. The main components, therefore, are a warrant system to authorise

---

[5] *Idem.*

intrusions, provision for their renewal or cancellation, the appointment of a senior judge as Commissioner, and the establishment of a tribunal to consider complaints. Section 3 of the 1989 Act provides that "no entry on or interference with property shall be unlawful if it is authorised by a warrant". Section 5 of the 1994 Act is wider and provides that a warrant can authorise any of the three secret services (MI5, MI6, and Government Communications Headquarters) to interfere with property, trespass on land or interfere with wireless transmissions. Under the regulatory scheme we are proposing, the types of interference applied for will have to correspond to the offences defined earlier in this paper.

Exceptions

Criteria for interception

6.28 We now examine the scope of public interest justifications for intrusions which would otherwise contravene the offences we have defined earlier prohibiting surveillance and/or the interception of communications. In formulating these public interest grounds justifying the issue of a warrant we have endeavoured to heed Lustgarten and Leigh' s exhortation that they constitute "precise and rigorous criteria . . . subject to careful and effective scrutiny after the event. "[6]

Security, defence and international relations in respect of Hong Kong

6.29 "Security, defence and international relations in respect of Hong Kong" is the phrase used in the Commissioner for Administrative Complaints Ordinance (Cap 397) and subsequently adopted in the Personal Data (Privacy) Ordinance. The test should be along the lines that the information would be of substantial value in safeguarding security, defence, and international relations.

Prevention or detection of serious crime

6.30 The United Kingdom Interception of Communications Act 1985 provides that a warrant may be issued where the intrusion is for the purpose of "preventing or detecting serious crime." The ambit of "serious crime" will first be examined, followed by the scope of "prevention or detection".

6.31 ***"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*

[6] Lustgarten and Leigh, *op cit,* at 46.

convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more."

6.32 While (b) is definite enough, (a) has been criticised for its vagueness. It is not at all clear how many people would constitute "a large number of persons". But it seems that many public order offences would be covered by the provision.

6.33 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 tapping will be authorised.

6.34 The comparable provision in the Australian Telecommunications (Interception) Act 1979 is both more restrictive and specific, with a core criterion of seven years imprisonment. The Barrett Review has recommended that this be reduced to three years, provided it also involves

"... two or more offenders and substantial planning and organisation; involves the use of sophisticated methods and techniques; and is of a kind ordinarily committed in conjunction with other like offences."[7]

6.35 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.

6.36 We have concluded that an offence punishable by a minimum of seven years imprisonment would adequately reflect the gravity of the offences we believe should justify the issue of a warrant. We accept, however, 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 our surveillance and interception proposals. **We therefore recommend that "serious crime" should mean either an offence punishable by at least seven years imprisonment, or an offence punishable by at least three years imprisonment where there is an element of bribery or corruption**. We acknowledge that there may be categories of offence other than bribery or corruption which those commenting on this paper may wish to add.

6.37 ***"Prevention or detection"*** It will be noted that the United Kingdom provision extends to the "prevention or detection" but not the "prosecution" of crime. The words "preventing or detecting such crime", and the significance of this omission were considered by the House of Lords in *R v Preston*[8]. In that case, five defendants were charged with importing drugs and sought access to prosecution evidence of

---

7 See Barrett, *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (1994), section 2.3.

8 [1993] 4 All ER 638.

intercepted conversations. They hoped that that evidence would establish duress and/or their innocence. The trial judge refused the defendants' request that they be provided with the transcripts, but nonetheless admitted them as evidence.

6.38 The House of Lords held 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.*"[9]

6.39 The Court considered that this conclusion also accorded with the stringent limitations on the retention of intercepted data prescribed by section 6 (discussed below).

6.40 The essential policy question is whether it is right that intrusions should only be legally sanctioned at the investigative stage. (The *admissibility* of materials obtained by surveillance/tapping is a separate issue considered below). We agree with the United Kingdom approach whereby intrusions should only be lawful up to, but not including, the prosecution of an offence. Otherwise the prosecution would be able to continually refine its charges up to the date of the trial. In practical terms we consider that the cut-off point between prevention/detection and prosecution is the laying of the charge. Police admittedly have considerable discretion as to the timing of this. Such a restriction would also accord with the present position whereby a suspect is not further interviewed once he has been charged. It also accords with solicitor-client confidentiality. However, additional warrants should be obtainable for intrusions to prevent or detect additional charges pertaining to the individual earlier charged.

6.41 **We accordingly recommend that a ground for issuing a warrant authorising intrusions should be that it is for the purpose of preventing or detecting serious crime.**

6.42 Other jurisdictions impose additional requirements before a warrant should issue. The two principal restrictions are that there is probable cause for suspicion and the information is not reasonably acquirable by other means. These requirements will now be examined.

---

[9] *Ibid,* at 666.

6.43 ***Probable cause*** The United States Wiretap Act requires that the authorising judge be satisfied that there is "probable cause for belief" that an individual has committed or is about to commit one of the specified serious offences. Similarly, under the German law "exploratory" interceptions are not permitted. 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,[10] it was subsequently omitted from the Act. Halsbury opines that it is nonetheless a precondition.[11]

6.44 We agree that intrusions should only be lawful in relation to individuals reasonably suspected of offending. These techniques should not be used for exploratory fishing expeditions. This is particularly so in view of the increased deployment of new technologies that facilitate telephone tapping with little effort, such as key word recognition.

6.45 ***Information which cannot reasonably be acquired by other means*** The United Kingdom Interception of Communications Act states that in determining whether a warrant is justified, a relevant matter is whether the information "could reasonably be acquired by other means".[12] The United States Wiretap Act is more explicit and 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."*[13]

6.46 The Canadian and German laws have similar provisions. The latter requires that other investigatory methods would be ineffective or considerably more difficult.

6.47 We also endorse this restriction that intrusions 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 surveillance. In particular, we support the rigorous provision of the United States law requiring the authorities to provide details of the difficulties which would arise from being restricted to conventional methods.

6.48 **We accordingly recommend that a warrant should be issued for the prevention or detection of serious crime only where:**

(a) there is probable cause for suspicion of the target; and

(b) the information is not reasonably available by less intrusive means.

---

10 *The Interception of Communications in the United Kingdom,* Cmnd 9438, 1985, para 20.

11 *Halsbury's Statutes*, vol 45, at 419.

12 Section 2(3).

13 *Op cit,* section 2518(1)(c).

Security, defence, or international relations

6.49 Probable cause for suspicion is less apt for security than crime. Hence sections 3(2)(a) and 5(2)(a) of the United Kingdom Security Service Act 1989 and the Intelligence Services Act 1994 respectively provide that the intrusion must be thought:

> *"necessary for the action to be taken in order to obtain information which ... is likely to be of substantial value in assisting the Service to discharge any of its functions; and cannot reasonably be obtained by other means"*

6.50 **We recommend a similar restriction on intrusions for the purposes of security, defence, or international relations in respect of Hong Kong. Intrusions should only be permitted where they are likely to be of substantial value in furthering security, defence, or international relations in respect of Hong Kong; and the information cannot be reasonably obtained by other means.**

6.51 ***Economic interests*** The United Kingdom Act also sanctions intrusions "for the purpose of safeguarding the economic well-being of the United Kingdom". During the Second Reading the Home Secretary said of this expression:

> *"As in the case of serious crime or national security the Secretary of State has to consider that interception is not just desirable. Secondly, interception has to be protective. It must be concerned with safeguarding the country's economic well-being, not with promoting it. That means it relates to threats to that well-being. Thirdly, it is the economic well-being of the United Kingdom which is at issue. By definition, the matter must be one of national significance and cannot be of a trivial kind which is peripheral to that well-being. It is a crucial part of our foreign policy to protect the country against adverse developments overseas, which do not necessarily affect our national security so directly as to justify interception on that ground but which may have grave and damaging consequences for our economic well-being, such as a threat to the supply of a commodity on which our economy is particularly dependent."*[14]

6.52 Lustgarten and Leigh comment that the wording is "broad enough to catch the actions of multinational companies, currency speculators, and the diplomatic communications of Britain's EC partners." It may be that this accords with current conditions: Peter Schweizer argues that with the end of the cold war secret services are

[14] 75 *House of Commons Official Report* 159, 160.

increasingly concentrating on 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, it has to be said . ... 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.*"[15]

6.53 Schweizer contends that such espionage is conducted by means of the usual clandestine techniques. Business executives and trade negotiators are bugged and tracked at home and abroad. Corporate telecommunications are regularly monitored and eavesdropped.

6.54 Notwithstanding the prevalence of such state sponsored industrial espionage, we think that a broad provision along United Kingdom lines would be inappropriate for Hong Kong. We believe, however, that the importance of protecting the Hong Kong currency peg to the US dollar merits special consideration. **We therefore recommend 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 should extend to intrusions conducted both within and outside Hong Kong.**

Duration of warrants

6.55 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. Section 4 of the United Kingdom Interception of Communications Act provides that warrants shall be issued for an initial period of two months and thereafter require renewal, also for a period of two months (but with provision for six months). Renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2. The United Kingdom's two secret service acts prescribe six months. Six months is similarly the period prescribed under the Australian Act for both security (section 9(5)) and customs (section 21(5)). The Canadian Act adopts 60 days. The United States Act is the most stringent: section: 2518(5) at 4 stipulates 30 days.

6.56 We think that 60 days should suffice for both crime and security. A similar period should govern extensions. We have considered but reject adoption of an upper limit to the number of extensions given. One possibility was that repeated extensions should be

---

[15] Peter Schweizer, *Friendly Spies,* (1993), at 13.

dealt with by a higher court. On the other hand, the initial determination of whether to approve a warrant is likely to be the most important determination. **We recommend that a warrant should be issued for an initial period of 60 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.**

Safeguards regarding retention of surveillance materials

6.57 Section 6 of the United Kingdom Act requires that the Secretary of State shall make such arrangements as are necessary to ensure that:

- the extent to which the material is disclosed
- the number of persons to whom any of the material is disclosed
- the extent to which the material is copied
- the number of copies made of any of the material

is "limited to the minimum that is necessary" for the purposes under section 2 (i.e. the prevention and detection of serious crime etc.). The case of *Preston* made it clear that this provision restricting the currency of intercepted material was only workable where the purpose of the interception and the retention of the resultant surveillance materials was restricted to the "preventing and detecting" of crime in the sense explained above:

> *"With the handful of people in the public service engaged in the use of intercepts for the forestalling and detection of crimes this makes sense, but if the purpose includes the prosecution of offenders it is impossible to imagine that any 'arrangements' made by the Secretary of State under section 6 which would prevent the materials from being liberated into the trial process, as happened in R v Effik, after which any attempt to control their wider dispersion would be hopeless, thus compromising both the secrecy of the interception process and the privacy of those whose messages had been overheard."*[16]

6.58 It became apparent during the trial in *Preston* (although no evidence was led to that effect) that the defendants' telephones had been tapped and the defendants sought access to material so derived to establish a defence (coercion). The Court held that section 6 required that intercept materials must be destroyed once police inquiries resulted in charges being laid, and it was this, rather than section 9's restrictions on admissibility (discussed below), which precluded the defendants from having the material admitted.

---

16 [1993] 4 All ER 638 at 667.

6.59 Accordingly, under the United Kingdom scheme, the "shelf life" of surveillance materials is strictly limited. The timing and specific purposes of intrusions must be specified in the warrant. Upon fulfilment of those purposes the material obtained pursuant to the warrant must be immediately destroyed and hence may not be used as evidence. The destruction of the material protects the privacy of targets and their contacts. Controls providing some accountability are provided at another level. The appeal of this approach is that it disposes of some basic difficulties which would otherwise arise from retention of the material. Such a system arguably sustains public confidence. The evidential implications are examined below.

6.60 **We recommend the adoption of provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985, including the imposition of a requirement on the warrant-issuing authority to ensure that adequate steps are taken to achieve compliance with the stipulations set out at paragraph 6.57 above**. Our adoption of provisions along the lines of section 6 will have the result that evidence of the fruits of *authorised* surveillance will never be available in a prosecution: their purpose has been spent in addressing the earlier stage of the fight against crime, namely prevention and detection, and must thereupon be destroyed. But as regards unauthorised surveillance, such materials would necessarily escape the statutorily imposed requirements regarding its destruction. Accordingly, such materials would be available as evidence in a subsequent prosecution. This question will now be examined.

Admissibility of surveillance materials

6.61 Under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence. There is, however, a judicial *discretion* to exclude unfairly obtained evidence. The United States law prohibits the admission of illegally obtained evidence and supporters of this approach argue that this both discourages illegal methods and concentrates the minds of investigators on more straight forward means of investigation. Deeming illegally obtained surveillance materials inadmissible would not preclude investigators from using it during the investigation, such as confronting suspects with the materials to elicit confessions.

6.62 Under the United Kingdom Act, these questions do not arise as regards telephone tapping because section 9 prohibits any reference to this intrusion, whether it is authorised or unauthorised. It provides that in any proceedings of a court or tribunal "no evidence shall be adduced and no question in cross examination shall be asked which tends to suggest" that an intercept has or will occur, whether authorised by warrant or not. It will be recalled that the genesis of this legislation was just such a question!

6.63 The court in *Preston* concluded that the "otherwise impenetrable" section 9 only made sense on the basis of a narrower interpretation of section 2:

> *"If the purpose of Parliament was to allow the intercept materials to become part of the prosecution process it is hard to see any point in a*

provision which would make it ... impossible to use them in that process ... . By contrast, on the narrower reading of s. 2 there would be no need to make explicit provision for the admissibility of materials which by virtue of s. 6 would no longer exist, and the purpose of s. 9 can be seen as the protection, not of the fruits of the intercepts, but of the information as to the manner in which they were authorised and carried out."[17]

6.64 In Hong Kong there is presently no bar to the defence raising the issue of tapping, provided it is relevant to the case. Usually, this would not be relevant, because it would relate to that part of the investigation which would be adequately referred to in the trial that as a result of "information received" the police were at the scene of the attempted crime. However, given the breadth of our proposed offences criminalising surveillance and the interception of communications, adoption of a provision along the lines of section 9 would have the effect of generally prohibiting the admissibility of evidence of all surveillance and interception activities. This is not the United Kingdom position, because there only the interception of communications is prohibited. Furthermore, even this prohibition has been narrowly defined. It will be recalled that in *R v Effik* an interception was effected without a warrant. The court concluded that no warrant was required because the interception was not prohibited, as it had been conducted outside a public telecommunications system. As such, section 9's restrictions were not applicable and the evidence, not being excluded by statute, was admissible. However, our much broader prohibitions on surveillance and interception of communications should catch intrusions across the board and a provision in similar terms to section 9 would render any reference to such activities inadmissible, whether or not it was authorised.

Deliberations on use of materials in prosecutions

6.65 Initially, we were disposed to agree that surveillance materials pertaining to the period preceding the laying of the charge should be able to be used in the subsequent prosecution. This was on the basis that it would help address the serious international crime problem facing Hong Kong. While evidence arising from intercepts is not usually admitted here, in a recent major drug case it was.[18] In that case, however, the calls were intercepted by the Royal Canadian Mounted Police. We also note that the United States, Canada, and Australia all countenance the admission of surveillance materials as evidence in prosecutions.

6.66 We recognise, however, use of surveillance/intercept materials as evidence will require their retention for this purpose. Furthermore, not only does this pose the risk of dissemination, but the inevitable outcome of their use as evidence. What is more, it is *public* dissemination which will result. In other words, use as evidence will necessarily seriously compound the invasion of privacy entailed by the original intrusion.

---

17 *Idem.*

18 *R v CHEUNG Kai-tai YEUNG Hing-yu,* CA 198/82, ruling on 22 August 1995.

6.67 In addition to this objection in principle, there are practical difficulties about retaining surveillance materials for use as evidence. Only a small part of such materials would be used by the prosecution and the remainder of the police evidence would have to be provided to the defence as unused material. It would be a matter for the court to impose appropriate conditions. For example, defence counsel may have to undertake not to divulge the contents of tapes played to them. The present legal status of unused materials is vexed and is subject to a number of appeals. A further complication which is avoided by prohibiting the use of surveillance materials as evidence arises from the application of public interest immunity.

6.68 **For these reasons, we recommend that materials obtained through surveillance or interception should be inadmissible as evidence, regardless of their relevance.** We accordingly reject any qualification of our endorsement of the United Kingdom Act's provisions whereby such materials will be destroyed once an investigation moves into prosecution mode. **Furthermore, we recommend the adoption of the United Kingdom's prohibition on the admission of evidence obtained by means of unauthorised surveillance or interception of communications. The prohibition should cover not only the fruits of surveillance but also details of methods used.**

6.69 We note that this approach apparently accords with existing Hong Kong practice. According to a press report the approach adopted in *Preston* accords with current practice in Hong Kong. It was reported in February 1992 that Acting Deputy Secretary of Security, Mr Clinton Leeks, told the Omelco Constitutional Development Panel that all interceptions were in connection with investigations and were not part of evidence-gathering for court cases.[19]

6.70 We think that a major advantage of adopting the United Kingdom requirement that surveillance and intercept materials be destroyed and hence unavailable as evidence is that this provides a significant disincentive to undertaking surveillance in the first place. However, in the next chapter we examine whether surveillance materials should be retained specifically to be provided to former targets following the cessation of surveillance.

---

[19] *South China Morning Post,* 26 February 1992.

Chapter 7

Notification following termination of surveillance

Summary

7.1 In the previous chapter we concluded that as a general rule surveillance materials should be destroyed once the investigatory phase has been completed. Several other jurisdictions impose a requirement that upon the termination of surveillance, the target should be informed of that fact. In principle, such a notification requirement should increase the accountability of those engaging in intrusions. In this chapter we examine the feasibility of such a requirement and reject it as impractical.

A notification requirement

7.2 A requirement that the subject of surveillance be notified of that fact once the surveillance has been discontinued is a feature of some but not all laws. Thus section 2518 of the United States Wiretap Act prescribes detailed procedures.[1] It is also a feature of the German law. Indeed one aspect of the German law which was challenged in *Klass* is that there was no requirement that the subject of surveillance 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 surveillance. This indicates that a post-surveillance notification requirement is desirable in terms of compliance with the Bill of Rights.

7.3 The basis of a notification requirement is two-fold:

- 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 tapping unnecessarily.

- The individual should be able to challenge the grounds on which the intrusion had been granted. Denying the subject of surveillance such information will tend to undermine the efficacy of these mechanisms enhancing accountability, such as complaints procedures and the provision of compensation awarded for

[1] *Op cit,* section 2518(8)(d).

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.

7.4 We also think that the public has a right to be told the extent to which intrusions were occurring, although this would also be addressed by public reporting requirements. The adoption of a notification requirement along the above lines would diminish the need for mechanisms at the stage when the warrant was approved, such as the participation of a friend of the court.

7.5 We recognise, however, that merely to inform an individual of the fact that he had been the subject of surveillance would be unhelpful. 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 the intercept materials themselves. We understand that under current Hong Kong interception arrangements often only key points will be abstracted and retained. Requirements regarding the destruction of intercept materials were considered above. Destruction of the intercept materials prior to notification would largely destroy the basis of the notification mechanism. We recognise that "destruction" is not an absolute concept in the digital age.

7.6 Furthermore, a notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of investigative agencies would not be diminished. The requirement would have to be couched in terms that, following the cessation of surveillance, the subjects 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. However, the traditional United Kingdom approach is that surveillance is necessarily clandestine and merely divulging that it has occurred would be prejudicial. This is indicated by the following passage in *Preston*:

> *"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. We need not consider to what extent this preoccupation with secrecy at all costs is soundly based for it has been treated as axiomatic for decades, if not longer."*[2]

7.7 This is one approach and may be referred to as the "clandestine imperative" - i.e. that people should be generally kept in the dark about the incidence of surveillance. The difficulty is that applying the "prejudice" test on this basis would effectively negate the requirement of notification. That requirement would be illusory, since notification would necessarily conflict with the clandestine imperative and would therefore never occur. If there is to be a requirement, it must be clarified and tightened up before its full implications can be assessed. There is the additional aspect of the content of the notification to the ex-target - should this be restricted to the mere fact of notification. or extend to other matters, including

---

2 [1993] 4 All ER 638 at 648, *per* Lord Mustill.

surveillance materials. This would also need to be determined by the application of an explicit prejudice test.

Clarification of the notification requirement

7.8 For the requirement to be meaningful, it would have focus on actual prejudice in the particular circumstances of the case. Such a test depends on whether the surveillance is in respect of the target or an innocent party:

- ***Notification of target*** Prejudicial in relation to the particular target could be defined to cover the situation where the target is likely to be the subject of surveillance in the future and notification is likely to make such surveillance more difficult. This approach would preclude notification of recidivist offenders, or those where there was a reasonable prospect that the investigation may be reopened in the future.

- ***Notification of innocent parties*** The most obvious grounds on which it would be prejudicial to notify innocent parties in particular cases is if they could be expected to alert the target. Another possibility is that the authorities may wish to tap the innocent party in order to further tap the target again and alerting the innocent contact may make this more difficult.

Practical problems of notification

7.9 The implications of applying a more rigorous notification requirement along these lines include the following:

- ***Prolonged retention of surveillance materials*** The provision of the fruits of surveillance/intercept following its cessation assumes that they are still in existence. Indeed, a robustly applied notification requirement would necessitate their retention for this purpose when all other purposes had been fulfilled. The difficulty with this is that the retention of surveillance materials has its own privacy risks. We have **recommended above adoption of** the United Kingdom **requirement** that the fruits of surveillance be destroyed immediately they have fulfilled their functions.

- ***Resource implications*** 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 above lines. As we explained above, consideration would need to be given to the extent of the information given to the ex-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.

7.10 There is also the question as to who should determine whether the subjects should be notified, and the contents of such notification. In the United States this is done by a judge.

7.11 We have proceeded thus far on the basis that decisions impinging on surveillance/interceptions should be capable of review. However, if decisions regarding notification are similarly to be reviewed the resource implications will be even greater.

7.12 We have recommended above that surveillance materials be inadmissible. We consider that there is less need for a notification requirement here than in those jurisdictions where surveillance materials may be produced at the trial. We note that in the United States and Canada the apparent practice is only to notify the public of the fact of surveillance. It is presumably due to this that those jurisdictions have not apparently encountered the difficulties we envisage may result from a more extensive notification requirement. We think that such a restricted notification requirement is of little benefit and that identifying the range of innocent parties meriting such notification remains problematic. Finally, we believe that the accountability aspect is more directly addressed by the warrant requirement.

7.13 **We accordingly reject a notification requirement**. In doing so, our main concerns are that such a scheme would have considerable resource implications, without a clear concomitant benefit. We examine in the next chapter additional mechanisms adopted elsewhere to increase accountability and control over the surveillance process.

Chapter 8

Compliance enforcement: supervisory authorities and remedies

Summary

8.1 There are differences of approach between jurisdictions to the regulation of surveillance. This chapter examines the position in a number of other jurisdictions and makes recommendations on the nature of a supervisory body, remedies, and reports.

Recommendations

8.2 A Justice of Appeal should be appointed as the supervisory authority to review the issue of warrants authorising surveillance or the interception of communications. The applicable criteria should be those of judicial review.

8.3 The supervisory authority should be empowered to:

- *review cases at the request of an aggrieved individual; and*
- *examine whether the warrant was properly issued and whether its terms have been complied with.*

8.4 The supervisory authority should furnish annually a confidential report to the Governor and a public report to the Legislative Council. There should be a statutory requirement that the following matters be covered in both reports:

- *the number of warrants authorised*
- *their average length and their extensions*
- *the classes of location of the surveillance i.e. domestic, business etc.*
- *the type of surveillance device used*
- *the number of persons arrested and convicted as a result of the surveillance or interception*

8.5 Compensation should be payable for unauthorised intrusions. In addition to damages for actual loss suffered, in line with the Personal Data (Privacy) Ordinance, there should be compensation for injured feelings. Punitive damages should be available. We do not consider that a separate complaints tribunal will be required to supplement the role of the supervisory authority.

1 OVERSEAS JURISDICTIONS

The United Kingdom

8.6 The Interception of Communications Act 1985 establishes two distinct authorities, namely a supervisory authority and a complaints Tribunal.

Supervisory body

8.7 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 generated by intercepts. The appointee shall be "a person who holds or has held high judicial office". In practice, the appointee has been a sitting judge.

8.8 In his annual reports, 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]

---

1 1995 Annual Report of the Commissioner, at paragraph 4.

2 Lusgarten and Leigh, *op cit,* at 63.

8.9 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 and to date no warrant has been found to fail it.[3]

8.10 In addition to this selection of a sample of warrants for close perusal, the Commissioner also refers 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]

8.11 Accordingly, in the section of the United Kingdom Commissioner's annual report headed "Errors", the last three reports commence that "the following errors have been brought to my attention." Whilst the Commissioner's confessional role may well be therapeutic to those that wish to avail themselves of it, Lustgarten and Leigh have grounds for their conclusion that:

> *" 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

8.12 Section 7 of the United Kingdom Interception of Communications Act establishes a complaints tribunal comprised of lawyers. Whereas the Commissioner's review duties are ongoing, the Tribunal's review role is based on complaints. Further, the Tribunal may only investigate any breach of the requirements of the Act where a warrant has been issued. Interceptions not sanctioned by any warrant are instead a criminal matter for investigation by the police, although there is no legal requirement that unauthorised interceptions be referred to the police. Even if they are, the police may themselves be the perpetrators.

8.13 The jurisdiction of the Tribunal is therefore limited to ascertaining whether a "relevant" warrant has been issued and, if so, whether there has been a contravention of the provision authorising its issue. Because warrants are in practice only issued following careful vetting, Ian 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 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 not be limited only to the investigation of authorised interceptions, but should extend also to unauthorised interceptions.

---

3 *Ibid,* at 62.

4 *Report of the Commissioner for 1992,* Cm 2173, 1993, para 7.

5 *Ibid,* at 63.

6 Leigh, *A Tappers' Charter?* (1986) *Public Law* 8, at 15.

Reports

8.14 As to a requirement to issue a report, section 8(2) merely states that the Commissioner shall annually make a report "with respect to the carrying out of his functions".

The United States

8.15 Section 2519 of the Wiretap Act[7] provides that within 30 days of the court's consideration of an application for a warrant (whether or not approved), the judge must report to the Administrative Office of the United States Courts detailing:

- number of applications for warrants
- number of warrants authorised, with a breakdown for different offences
- the average length of authorisations and their extensions
- the total number of days that intercepts were actually in operation
- location of surveillance (i. e. private dwellings)
- average number of intercepts per day, the number of persons intercepted, the total number of communications intercepted, and the number of incriminating intercepts
- the type of surveillance device used
- the costs of installing devices and monitoring communications
- the number of persons arrested and convicted as a result of intercepts (i.e. the yield of this expensive investigative technique)

8.16 Subsection (2) provides that, similarly, the prosecuting authority must report annually covering not only the above details, but also the yield of incriminating communications, arrests, trials and convictions resulting from interceptions. Also required are details of the nature and cost of manpower and other resource expended used in interceptions.

---

7 *Op cit.*

8.17 Having received this data, the Director of the Administrative Office of the United States Courts in turn is required to provide Congress with an annual report giving the numbers of applications for orders and the number granted/denied, together with an analysis of all the other above matters that the judges and prosecution authorities must furnish. The reports are very detailed but a useful statistical analysis is provided by Statistics Department.

Remedies

8.18 As under its data protection regime, the United States provides no administrative mechanisms channelling complaints about intrusions. It is up to the individual to litigate: section 2707 provides a civil cause of action for any intentional breach of the enactment. It is a defence that there was a "good faith reliance on" a court warrant or order etc. Other non-constitutional remedies are ousted.

Australia

8.19 Sections 80 and 81 of the Telecommunications (Interception) Amendment Act 1987 require the prosecuting authority to record a similarly comprehensive class of matters to that required under the United States law. The Australian legislation does not establish its own supervisory authority. Instead it confers the review function on the Commonwealth Ombudsman. Unlike his Hong Kong equivalent, the Commissioner for Administrative Complaints, 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.[8] Clearly this role does not restrict him to the investigation of *authorised* taps, unlike the United Kingdom Commissioner. However, under the Telecommunications (Interception) Amendment Act 1987 he has the additional specific function of inspecting government records at least twice annually to ascertain compliance with reporting requirements and the destruction of intercept materials. For the purposes of such an inspection, the Ombudsman has powers to enter premises and be furnished with records. He also has powers to obtain information from officers of the agency. These investigative powers resemble those conferred on the Privacy Commissioner and the Commissioner for Administrative Complaints in Hong Kong and are absent from the United Kingdom Interception of Communications Act.

Remedies

8.20 The 1994 amendment to the Australian Act provides a civil remedy for *unauthorised* interceptions. Such claims must be pursued in court.

2 THE OPTIONS

[8] See the chapter on "Ombudsman" in Flick G A, *Federal Administrative Law* (1984), vol 2.

8.21 The following section summarises the differences noted above between the three selected jurisdictions, identifies the main options for regulating surveillance, and states our conclusions.

Supervisory Authority

8.22 Whereas the United Kingdom and Australia have a specially constituted administrative body tasked to monitor the application of the approvals system, in the United States the relevant authority 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.

8.23 As between the United Kingdom and Australia, the latter' s Ombudsman is full-time (as are his subordinates) but intercepts are only one of his office' s concerns. The United Kingdom Commissioner is part-time but in that capacity focuses solely on supervising intercepts. Our recommendations, however, cover not only interceptions but also surveillance and this will generate more work.

Deliberations on need for and role of supervisory authority

8.24 We consider that a monitoring body is necessary. A requirement that the subject of surveillance be subsequently notified of that fact would reduce review issues in those cases. Notification would equip the individual with explicit grounds to challenge the issue or application of the warrant. However, we rejected above a notification requirement and the issue of independent review therefore becomes crucial: as the individual will not be in a position to challenge the surveillance it is essential that another party scrutinise the matter on his behalf.

8.25 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 Privacy Commissioner and the Commissioner for Administrative Complaints. The Privacy Commissioner' s duties do have a nexus with surveillance and interceptions, in that it would sometimes be apparent from personal data that they have been compiled as a result of surveillance or the 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 act as the dispassionate friend of the data subject in ensuring fair play in data processing. The role of reviewing the authorisation of intrusions is different, and no other jurisdiction confers this additional role on their data privacy commissioner. 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 for the Secretary for Security. Saddling the Privacy Commissioner with the role of reviewing the issue of warrants would significantly alter his present statutory role and public perceptions of it. The existing duties of

the Commissioner will already prove taxing for an incumbent. The person reviewing the issue of warrants will play a pivotal role in securing law enforcement and security interests and would require a very 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 satisfied both the data protection lobby and the law enforcement/security community would be very difficult.

8.26 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. Such a decision would have to be made pursuant to an ex parte application. As ex parte applications are held in secret there is generally a right vested in the excluded party to have the order subsequently discharged. The review of whether a warrant had been properly issued would necessarily also have to be decided by a judge**,** albeit one more senior. We believe that this supervisory function should be concentrated instead of dispersed to enable the authority to obtain an overview of the incidence of surveillance throughout society, such as whether any particular segments were being targeted.

8.27 **We accordingly recommend that a Justice of Appeal should be appointed as the supervisory authority to review the issue of warrants authorising surveillance or the interception of communications. The applicable criteria should be those of judicial review.**

8.28 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 requirements had not been properly applied, or because the supporting affidavits may be false - a not uncommon occurrence in Hong Kong with Anton Piller applications.

8.29 We think that it should be left to the supervisory authority to determine which warrants he should examine and on what basis. There would in any event be judicial review proceedings open to individuals who became aware of the issue of the warrant, as well as proceedings for damages. **We also recommend that the supervisory authority should be empowered to review cases at the request of an aggrieved individual.**

8.30 **Apart from the question of whether the warrant has been properly issued, the other area for supervision relates to whether the warrant had been complied with. We recommend that this area should also be dealt with by the supervisory authority.**

Jurisdiction of supervisory authority

8.31 The United Kingdom Commissioner for interceptions is solely concerned with whether *authorised* taps have complied with statutory requirements. Furthermore, he

accepts that if interception without authorisation under a warrant were taking place, there would be no reason for such conduct to come to his attention.[9]. The Australian Commonwealth Ombudsman is not subject to this restriction and would be entitled to investigate unauthorised taps. Nonetheless, he is not specifically tasked to endeavour to detect such taps, nor would he be equipped to do so.

Deliberations on jurisdiction of supervisory authority

8.32 We were initially disposed to endorse the need for the supervisory authority to pursue allegations of improperly issued warrants, or intrusions not sanctioned by a warrant. To initiate such an inquiry, however, the supervisory authority would need grounds for believing that there had been a contravention of the statutory requirements. As it is impossible to eliminate the possibility of technical surveillance, mere suspicion would not suffice. Nor would the authority be itself equipped to investigate whether unauthorised intrusions were occurring. In any event, such unauthorised intrusions would be a criminal matter for investigation by the relevant law enforcement agency. In practice then, the supervisory authority would be restricted to checking the paperwork provided by the relevant agency. If that were the case, the only issue would be whether a warrant had been issued and, if so, whether it had been issued on proper grounds. Improper issue would usually be attributable to false supporting affidavits. We note that the effective exclusion of the investigation of unauthorised warrants coincides with the United Kingdom position, which becomes explicable on this basis. We have therefore concluded that the supervisory authority should be restricted to investigating whether a warrant had been properly issued.

Reports

8.33 All three jurisdictions discussed above endorse a degree of transparency about interception activities. This is achieved by publishing statistics on the number of authorised taps. The only data provided by the United Kingdom Commissioner's annual report is the number of authorised taps. The Commissioner has repeatedly said that the number of warrants is a misleading guide to the number of lines tapped, but has declined to indicate the number of people affected.[10] The figures on taps 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 very detailed (and graphic) picture. As a result, United States citizens and administrators are given a full picture of the incidence, cost, and effectiveness of intercepts engaged in for law enforcement purposes. Those engaged in such intrusions are accordingly accountable.

Deliberations on reports

---

9 *Ibid,* at 64.

10 *Ibid,* at 60.

8.34 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 surveillance. **We therefore recommend that the supervisory authority should furnish annually a confidential report to the Governor and a public report to the Legislative Council.** Unlike section 8(8) of the United Kingdom Act, however, we prefer to specify the different matters which must be included in the reports. The United States report focuses on the cost effectiveness of interceptions, but in our view this cannot be assessed in purely financial terms. Intercepts are becoming increasingly cheap and the more relevant cost is that of the intrusion into the individual' s privacy. The privacy costs to the community would be indicated by figures on the number of persons intercepted and the number of communications intercepted. **We therefore recommend that there should also be a statutory requirement that the following matters be covered:**

- **the number of warrants authorised**
- **their average length and their extensions**
- **the classes of location of the surveillance, i.e. domestic, business etc.**
- **the type of surveillance device used**
- **the number of persons arrested and convicted as a result of the surveillance or intercepts.**

8.35 We consider this last item important because it would indicate the yield of the intrusions and would make the authorities accountable to the community regarding their utility. If large scale surveillance was resulting in few arrests or convictions the community would be entitled to question whether the privacy costs were justified by the results.

8.36 The confidential annual report to the Governor would cover such matters as were 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.

Operational implications

8.37 In *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."[11]

"... the purpose of s. 9 [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."[12]

8.38 Even accepting the rationale of this approach, we do not think that publication of informative reports along these lines will "diminish the value" of surveillance activities. Because the figures are 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 people should know the extent of surveillance in their society.

Remedies

8.39 In our view, the United Kingdom' s provisions for monetary compensation[13] are illusory. They are restricted to breaches of statutory requirements in the issue of warrants. Unauthorised taps are not compensatable. Not surprisingly, no compensation has been awarded to date by the specially constituted tribunal. Both the United States and Australian laws provide aggrieved parties with a statutory right to claim in court monetary recompense for unauthorised intercepts.

Deliberations on remedies

8.40 For reasons given above we doubt the feasibility of investigating whether unauthorised surveillance has been conducted. Nonetheless, whilst it would be unusual for an individual to learn that he had been subject to unauthorised surveillance, this would happen from time to time. **We recommend that compensation should be payable for unauthorised intrusions. Providing for compensation provides an additional sanction and provides both a norm and a deterrent. In addition to damages for actual loss suffered, in line with the Personal Data (Privacy) Ordinance, there should be compensation for injured feelings. Punitive damages should be available.**

Supervisory tribunal

8.41 In addition to establishing a supervisory authority, section 7 of the United Kingdom Act establishes an independent tribunal to investigate complaints regarding the

---

11 [1993] 4 All ER 638 at 648.

12 *Ibid,* at 667.

13 Interception of Communication Act 1985, section 7(5)(c).

issue of warrants. A person who believes himself the subject 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 police matter.

8.42 Our reasons for concluding that it is not feasible for the supervisory authority to investigate unauthorised surveillance apply equally to a complaints tribunal. Furthermore, we have recommended that the supervisory authority be empowered to pursue complaints. Finally, we have recommended 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.**

Chapter 9

Legal and policy issues arising from the impact of encryption and other new technologies

Summary

9.1 This chapter examines the impact of new technologies on the ability to tap into telecommunications systems, and the competing ability to encrypt messages. There are at times opposing interests in, on the one hand, the individual's desire to ensure his privacy and, on the other, governments' need to access telecommunications for legitimate purposes, such as the prevention of serious crime. The chapter looks at proposals in the United States to create a government encryption standard that would facilitate the government de-scrambling encrypted voice communications.

Introduction

9.2 The discussion so far has assumed that telecommunications are always capable of interception. However, as a result of new technologies, interception efforts may be thwarted. This creates a dilemma. A tension exists between the growing need for communications privacy in today's global competitive environment and the need for access to communications by law enforcement and security agencies. There are two main aspects of this issue of telecommunications interceptability (TI), namely "tappability" and encryption:

- *"tappability"*: Some new technologies (e.g. optical fibres) are making it harder to tap into telecommunications systems and intercept messages.

- *encryption*: even where the communication is intercepted, modern technical developments in cryptography may preclude it from being deciphered. The purpose of cryptography is the encrypting (i.e. scrambling) of information. There is now easy availability of encryption sufficiently strong that an encrypted message would take the world's most powerful supercomputer years to crack. The dilemma arises from the fact that, as the White House put it upon its announcement of the "Clipper Chip" scheme discussed below, encryption is "a dual-edged sword" that helps to protect the privacy of individuals and industry, but also can shield criminals and terrorists.

9.3 Both these aspects of TI raise similar policy issues regarding the competing need for privacy and security of telecommunications on the one hand and effecting interceptions in the public interest on the other. Following the statement of these general principles applicable to TI generally, we will examine the specific issues relating to tappability and encryption respectively. In the final analysis, however, the two issues are linked, as the greater the extent to which encryption precludes the deciphering of communications, the less important becomes the issue of whether the communications can be intercepted in the first place.

Increased need for privacy in a networked world

9.4 As discussed in the introduction, 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. Also relevant are the concerns of the global marketplace: the need for security of communications in such areas as banking and theft of proprietary information are two such concerns. Security is the "key component for the continued success of the information highway" Proposals that limit privacy and security of communications will ultimately slow the development of advanced networks.

The need for balance

9.5 Governments face a fundamental tension between two competing policy objectives: (i) fostering the development and widespread use of cost-effective information safeguards, and (ii) controlling the proliferation of safeguard technologies that can impair signals intelligence and law enforcement capabilities.

9.6 The complexity of the issue is compounded by the large number of "stakeholders". The following United States list of parties with a stake in effective encryption would apply to TI issues generally:

- the government for its own operational needs
- the defence establishment, including security and intelligence functions
- law enforcement, not only for its own security needs but also for counter-intelligence against law-breakers
- private sector corporations protecting corporate secrets and communications. For certain industries, such as banking and financial services, communications security is critical.
- society at large as users of telephony and data networks requiring confidentiality
- the academic community in pursuit of study and research

9.7 The conflicting interests of so many stakeholders inherent in TI issues can impede effective debate. The conflict can be crudely grouped between government/law enforcement/defence on the one hand and corporations, society at large and the academic community on the other. To the extent that TI exists/is maintained, it facilitates not only bona fide interceptions for, for instance, law enforcement purposes, but also unlawful interceptions by criminals, terrorists, spies and hackers.

The claim to intercept

9.8 Legislation protecting the privacy of telecommunication systems is invariably accompanied by the securing of interception capabilities for public interest purposes. For example, the United Kingdom Home Office report preceding the enactment of the Interception of Communications Act noted the need to protect telecommunications systems whilst staking a claim to effect intercepts:

> *"The Government believes that the properly controlled interception of communications for certain limited but important purposes is not only justified but essential in the public interest. ... If normal methods of investigation are not available, it is right that means should exist to obtain information about such activities through the interception of communications, so long as this is carried out under clear safeguards and strict controls. ... The Government's aim in introducing legislation is to provide a clear statutory framework within which the interception of communications on public systems will be authorised and controlled in a manner commanding public confidence."*[1]

9.9 We accept that the interception of communications is an important investigative technique. The United States Federal Bureau of Investigation ("FBI") asserts that during the period 1985 to 1991, court-ordered electronic surveillance led to 7,324 individuals being convicted, fines of $295 million being levied and the saving of $1.86 billion in potential economic loss. These figures are derived from their annual reports which, unlike those of the United Kingdom, provide a detailed financial analysis of expenditure and law enforcement yields.

The claim for *effective* interceptions

9.10 More contentious is the more recent claim that such interception efforts be *effective*. The nature of a claim by law enforcement agencies to maintain TI requires scrutiny. Is it a matter of operational expediency, or does it have a specific legal basis? It has been pointed out that there is nothing inherently illegal or suspect about the use of the telephone. Nor have we reached the stage where taking steps to protect privacy such as by encrypting our voice or data communications suggest that we have something to hide. United States critics view interceptions as analogous to the State's rights of search and seizure and point out that such powers are in terms that guarantee the success of a search:

---

[1] *The Interception of Communications in the United Kingdom,* Cmnd 9438, 1985, paras 4-7.

> *"As is widely noted, there is a fundamental similarity between the power of the government to intercept communications and its ability to search premises. Recognising this power, the fourth amendment places controls on the government's power of search and similar controls have been placed by law on the use of wiretaps. There is, however, no suggestion in the fourth amendment of a guarantee that the government will find what it seeks in a search. Just as people have been free to protect the things they considered private, by hiding them or storing them with friends, they have been free to protect their conversations from being overheard."*[2]

9.11 A legal concept that is marginally relevant in this context is the privilege against self-incrimination. This would be more so where the interception law countenances the use of intercept materials as *evidence* in prosecutions. Our proposals, however, specifically prohibit their retention and use for this purpose.

9.12 On the other hand, the United States FBI claims that it seeks "to preserve the status quo for the criminal law enforcement community in terms of its current and past ability to carry out ... authorised electronic surveillance". In view of the discussion below, however, a more accurate assessment would be that it wishes to benefit from new technologies enhancing its "current or past" surveillance capabilities, whilst neutralising new technologies undermining such capabilities. While, therefore, reference to "preserving the status quo" is incomplete, the fact remains that some communications relevant to law enforcement will become more difficult or even impossible to intercept.

The impact of new technologies

9.13 The impact of new technologies on tappability is mixed. Certain technological developments are making it more difficult to isolate individual communications. An example is the replacement of copper wires with fibre optics which can carry thousands of conversations in a single strand of fibre. In the Hong Kong context, we doubt if this would present problems for authorised intercepts. This is because our telecommunications system is completely digitalised and we understand that taps are effected by means of switching software. In the United States a 1994 survey of several FBI offices found "no instances in recent years in which FBI agents had encountered any technology-based problems in conducting wiretaps."[3] This accords with information obtained under the Freedom of Information Act in relation to the FBI's telephony initiative. This disclosed that

---

[2] *Key Escrow: Its Impact and Alternatives - Testimony of Dr Whitfield Diffie before the Subcommittee on Technology and Law of the Senate Judiciary Committee*, 3 May 1994, page 3, collected in Electronic Privacy Information Centre ("EPIC"), David Banisar (ed), *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls* (Diane Publishing, Upland, Pennsylvania, 1994), Part II.

[3] New York Times, 1 March 1994

as at December 1992 law enforcers were not experiencing technical interception problems caused by advanced telephony technology.[4]

9.14 Other developments make for *increased* vulnerability to intercepts. Major examples in telecommunications include:

- the rising demand for mobility in communications using radio communications
- modern communications systems, like ISDN, provide much more information about each call, revealing the origin of the call and so enabling patterns of conduct and contacts to be identified

9.15 One distinguished commentator argues that "on balance, it appears more likely that the investigative and evidential utility of wiretaps is rising than that it is falling." He adds that "this is partly because criminals, like law abiding citizens, do more talking on the phone these days."[5]

9.16 Nor should telecommunications surveillance be looked at in isolation. Other kinds of electronic surveillance provide law enforcement with increased opportunities. Miniaturisation of electronics and improvements in digital signal processing are examples and the proliferation of surveillance technologies generally is described earlier in our report.

9.17 At the institutional level, the increasing complexity of the telecommunications infrastructure tends to make for more dispersed interception efforts.

9.18 Assuming that some interception capabilities either are, or will shortly become, eroded, the issue arises as to what should be done. The United States approach has been to legally mandate tappability. An examination of their legislation indicates some of the problems arising from this approach.

The US Digital Telephony and Communications Privacy Improvement Act 1994

9.19 Initially proposed by the FBI in March 1992 and approved by Congress in October 1994, this legislation for the first time requires that telecommunications systems must be designed to facilitate government interception. It provides that:

> "*Common carriers shall be required to provide forthwith, pursuant to court order or lawful authorization, the following capabilities and capacities in order to permit the government to conduct electronic surveillance and pen register and trap and trace investigations effectively:*

---

4 *Privacy Journal,* December 1993

5 Whitfield Diffie, *op cit*.

(1) the ability to execute expeditiously and simultaneously within a common carrier's system all court orders and lawful authorizations for the interception of wire and electronic communications and the acquisition of call setup information related to the facilities or services of subscribers of such common carrier;

(2) the ability to intercept the content of communications and acquire call setup information concurrent with the transmission of the communication to or from the subscriber's facility or service that is the subject of the court order or lawful authorization, to the exclusion of any wire or electronic communication or call setup information of any other subscriber ..."[6]

9.20 The legislation avoids the difficulties of making the internet interception-friendly by excluding such on-line information services, together with electronic messaging services, and electronic publishing. However, it does provide for a subpoena process for obtaining customer information on such on-line services.

9.21 Before proceeding with legislation the United States administration considered but rejected a voluntary approach. The Director of the FBI explains that:

"A legislative approach was presented to the President because the telephone service and switch manufacturing companies indicated they would not design and implement a solution absent legislation forcing all companies to do the same, i. e. to 'level the playing field'."[7]

9.22 Concerns about the implications of the legislation include those relating to security, impact on the role of service carriers and cost.

9.23 ***Security*** It has been remarked that:

"The proposed legislation [requiring system modifications] would assist eavesdropping by law enforcement, but it would also apply to users who acquire the new technology capability and make it easier for criminals, terrorists, foreign intelligence (spies) and computer hackers to electronically penetrate the phone network and pry into areas previously not open to snooping. This situation of easier access due to new technology changes could therefore affect national security."[8]

---

6 Digital Telephony and Communications Privacy Improvement Act 1994, section 3(a), reproduced in EPIC, *1994 Cryptography and Privacy Sourcebook, op cit,* Part III.

7 Director, FBI, *Memorandum on Digital Telephony - Request for Briefings by the Special Agents in Charge,* 23 March 1992, collected in EPIC, *1994 Cryptography and Privacy Sourcebook, op cit,* Part III.

8 General Services Administration, *Comments on FBI Digital Telephony Proposal,* collected in EPIC, *1994 Cryptography and Privacy Sourcebook, op cit,* Part III.

9.24 ***Impact on the role of service carriers*** The President of the United States Telephone Association has criticised the legislation's potential impact on the role of service carriers. Noting the hitherto co-operative working relationship that exists between telephone companies and law enforcement, he said that such legislation:

> *"forces local exchange carriers to become, in effect, agents of the law enforcement community, rather than maintaining the more appropriate arms-length relationship between common carriers and law enforcement."*[9]

9.25 ***Cost*** Also of concern are the costs incurred by telephone companies for necessary technical conversions of their switches and computers. This has been estimated at between US$500 million and US$1.8 billion. The legislation requires the government to reimburse the telephone companies. The public may intervene in proceedings before the Federal Communications Commission concerning telephone companies' measures to alter their technology and resultant costs.

Australia

9.26 A different approach has been adopted in Australia. In 1990 the Australian Cabinet determined that all public telecommunications services should be capable of being intercepted for law enforcement and national security purposes. In 1991 licence declarations were amended to require that a licensee must not operate a telecommunication network unless:

- it is possible to execute a warrant under the Telecommunications (Interception) Act 1979 in relation to a telecommunications service provided by that network; or

- if it is not possible to execute such a warrant (there being no legislative constraint on the manufacture and use of encryption devices in Australia), the Minister, after consultation with the Attorney General, authorises the licensee's operation. Authorisations have been issued under this provision.

9.27 Notwithstanding this legal framework, the Australian Barrett Report[10] specifically rejects legislation along United States lines imposing a unilateral requirement that carriers/service providers only introduce technology that is interceptable. It reasons that "such a unilateral policy runs the risk of implementing less than world class technology which could put Australia at a major disadvantage in a cost sense". However, "the sooner an *international* requirement for interception is standardised and accepted, the more likely there will be the automatic provision of TI capability in new technology with similar

---

9 *Prepared Testimony of Roy Neel before the Senate Judiciary Subcommittee on Technology and the Law*, 18 March 1994, collected in EPIC, *1994 Cryptography and Privacy Sourcebook, op cit*, Part III.

10 *Op cit,* at 6.

implications for all users". Barrett expects it to take 3 to 8 years for such an international agreement to be reached.

9.28 On this question of maintaining tappability, we note the Barrett Report's view that unilateral policies were not financially sensible. In any event, we consider that the relevant issue is the imposition of legal controls authorising tapping. The question of controls on technology to maintain tappability subject to such authorisation is outside our terms of reference. Furthermore, we think that the issue of tappability is subsidiary to that of encryption: it matters not if a communication can be intercepted but nonetheless cannot be decrypted. We accordingly now examine the issue of encryption.

Encryption

Encryption: the most important privacy technology

9.29 The impact of new technologies on the capability to *intercept* communications is therefore mixed. However, the interception objective is usually to comprehend the communication (although sometimes identifying the parties may suffice). At this second level, namely deciphering the communication, the impact of technical developments is less equivocal: encryption is now capable of effectively preventing the interceptor from understanding the communication. For example, it is estimated that it would take 20 years for a super-computer to decode a communication utilising the Clipper Chip.

9.30 Encryption is the single most important technology for the protection of privacy. In the last 5 years, encryption technology has become easily available to both individuals and businesses. This availability will accelerate with the continued expansion of the Internet with its capacity to disseminate strong cryptographic software.

9.31 Accordingly the public is likely to become increasingly concerned about cryptographic policy. The development of the Global Information Infrastructure will heighten these concerns.

Encryption as an accessible tool

9.32 Encryption software can be generated in less than 5 minutes with such simple equipment as PGP ('Pretty Good Privacy") software for e-mail and PGP Fone software for speech over a network using 2 Power Macintosh computers. PGP is the most popular system, being freely available to United States citizens in the United States and freely outside the United States, where it is not subject to patents. It is believed that the system is strong enough to resist challenge from most quarters, although it is impossible to prove how strong the system is, only how weak.

9.33 A vital feature of modern cryptography is that of the public keys. A lock-and-key approach is adopted to telecommunications security. The lock is a "public key", which a user can transmit to recipients. To unlock the message, the recipient uses a

personal encryption code or "private key". The development of public key cryptography in the mid-1970s eliminated the need for network subscribers to provide trusted elements with the capability of decrypting any message. Public key encryption dramatically increases the availability of encryption/identification as the dual key system allows the encryption key to be made available to potential communicants while keeping the decryption key secret. This would allow, for example, a bank to make its public key available to many people, without those people being able to read each others' encrypted messages. Two relevant limitations, however, are:

(i) keys infrequently changed have an increased risk of being broken as, in principle, any public key system can be broken given sufficient computer power and time.

(ii) it is critical to ensure that the user has the correct public key. If provided by an intermediary, he could interpose a key of his own. Hence trust is a critical issue.

9.34 Another important feature of encryption is key signatures. These verify the identity of the person sending the message. They can be wiped after sending the message, so rendering it anonymous.

9.35 A system popular in the Hong Kong telephone market is that of Global System for Mobile communications (GSM) phones. The digital GSM technology employs a 54 bit encryption code: a single call would take a Cray supercomputer two hours to decipher.

The background to the debate: the Clipper Chip proposal

9.36 The public debate on the privacy and policy issues arising from cryptography has been largely generated by the development of the "Clipper Chip". On 16 April 1993 President Clinton's press secretary announced "a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement." Clipper is a hardware microcircuit based upon the classified "Skipjack" encryption algorithm (an algorithm is the rule by which an encryption scheme works) developed by the United States National Institute of Standards and Technology to scramble telecommunications. The Clipper Chip would create a government encryption standard that would facilitate the government descrambling voice communications encrypted with the chip, thus constituting an electronic "trapdoor" facilitating government eavesdropping on digital communications. The chip could be used in relatively inexpensive encryption devices that can be attached to an ordinary telephone. While the Clipper chip applies encryption to voice messages, "Capstone" is the related scheme for the encryption of data.

9.37 The official announcement of the scheme emphasised that the proposal only provides a new technology for tapping, not an extension of legal authority to do so. The Clipper proposal also acknowledged that public acceptance would require that the

Government must be trusted not to abuse the proposed capability to decrypt private transmissions without judicial warrant, as presently required. The proposed scheme to ensure this is known as "key escrowing" i.e. the means of decrypting a Clipper conversation. Two "trusted third parties" are designated who each hold a piece of the decryption key. The communication can be decrypted only by obtaining both pieces of the decryption key, pursuant to legal authorisation. The government initially favoured one of the third parties being non-governmental. However, private organisations were reluctant to accept the responsibility and in February 1994 the United States administration identified the Treasury and the National Institute of Standards and Technology as assisting in holding the keys.

9.38 The Clipper scheme has generated great controversy, with 80% of Americans polled expressing opposition, widespread business opposition, and an Internet petition opposing it gathering 47,000 signatures in one month.[11] Many of the concerns surrounding the Clipper chip focused on whether that encryption standard will become mandatory for government agencies or the private sector, if other encryption will be banned, and/or if these actions could be taken without legislation. The major commercial objection was that foreign users of telecommunications equipment would not purchase United States equipment loaded with Clipper Chips because it would provide United States government agencies with a "back door" to all their electronic communications. The Business Software Alliance, for example, predicted it could cost United States business US$9 billion per year in lost sales.

9.39 Accordingly, it was reported in October 1994 that Congressional representative Maria Cantwell had negotiated an agreement whereby the administration decided to "move beyond Clipper". Government agreed to accept seven key principles as the framework to develop an encryption system. It should be voluntary; exportable; not rely on a classified algorithm; implementable in software; firmware; hardware or any combination; permit the use of private-sector key escrow agents contain safeguards to provide key disclosure only by court orders, with audit procedures; and hold escrow holders liable for unauthorised key release.

Controls on encryption

9.40 Whilst encryption would appear to pose obstacles to investigative efforts, it appears that any threat to TI is potential rather than actual: the Barrett Review concluded in 1994 that Australian law enforcement agencies "do not currently consider encryption as a significant threat to interception".

9.41 We believe an encryption policy which does endeavour to tackle any future erosion of TI must recognise that prohibiting encryption is unenforceable. It is futile for Hong Kong to endeavour to unilaterally suppress hardware and software with encryption capabilities because:

---

[11] *The International Privacy Bulletin,* July 1994

- sophisticated encryption products are becoming available world-wide

- any person owning a modem and a computer can obtain encryption software through the Internet, usually free

9.42 Accordingly we do not consider that it would be feasible to promulgate a standard such as the Clipper chip providing trapdoor access to government agencies and wait for it to become a *de facto* standard within Hong Kong. We do not believe that this scenario is plausible even for the United States, the international leader in computer standards because international companies would not accept it. Hong Kong is too small to proceed down the Clipper chip path. The Clipper chip battle will be fought between the United States and Europe: even if the United States does impose an encryption key providing it with backdoor access, it is unlikely such a standard will be embraced by Europe. Hong Kong imports all its switching equipment, both hardware and software. It is not presently feasible for the territory to enforce the use of products solely for use in Hong Kong.

9.43 Similarly, it would be futile to promote a voluntary encryption standard providing law enforcement with a "back door" access (e.g. the Clipper chip) while other standards without such access remain available, as criminals and terrorists, etc., will naturally resort to the latter. Unless everyone uses the encryption code, the entire effort is futile.

Encryption and tappability

9.44 In our view, once encryption becomes generally available, the issue of tappability becomes less important, as even when intercepted, the encrypted communication will be indecipherable. We expect that that encryption will become so available, thereby securing privacy of telecommunications for those wishing to avail themselves.

Limits on encryption as a safeguard

9.45 Whilst encryption may indeed be unbreakable, it does not follow that encrypted data will necessarily be safeguarded. As a recent review puts it: "the strength of an encryption algorithm often has little to do with the actual security of encrypted data". The reason given is the growing resourcefulness in using technology for illegal purposes. For example:

> *"Recently, an automated teller machine was placed in a mall in New York by some persons who had programmed the machine to extract the customer's PIN along with the account number from the magnetic stripe on the bank card and return a null transaction. The thieves were then able to withdraw any sums they desired from the unsuspecting bank customers' accounts. ... Makers of ATM machines insisted that passwords and other data must be DES encrypted to protect against criminals, and ATM machines are in fact licensed for export with DES encryption. The result was that criminals took the imaginative and*

expensive route of building a phony machine to get the data they wanted."[12]

[12] *Draft Report on Impacts of Telecommunications and Encryption Technology on Law Enforcement and Intelligence Collection: Assessment, Options, and Recommendations, attached to memorandum of US National Security Council,* 19 November 1993, collected in Electronic Privacy Information Centre, *1995 EPIC Cryptography and Privacy Sourcebook: Documents on Encryption Policy, Wiretapping, and Information Warfare* (Diane Publishing, Pennsylvania, 1995), at page C-46.

Chapter 10

Other approaches to regulating intrusions: licensing

Summary

10.1 This chapter examines the possibility of licensing as a means of controlling surveillance and interception. The two possiblities considered are the licensing of surveillance equipment itself and the licensing of private detectives.

Recommendations

10.2 We do not recommend the licensing of surveillance equipment. We consider the question of licensing of private detectives beyond our terms of reference and make no recommendation on that option.

Licensing of surveillance equipment

10.3 Chapter 3 considered Hong Kong licensing restrictions on the possession or use of surveillance devices are imposed by section 8 of the Telecommunication Ordinance (Cap.108). We noted that a wide variety of scanners and receivers are available in Hong Kong, apparently sold on the understanding the buyers are tourists and the equipment will be exported. Some 50 shops are reported to be selling surveillance equipment in Tsim Sha Tsui and Central alone.[1]

10.4 **In view of this apparent lack of effectiveness of existing controls on the availability of surveillance equipment, we are unable to recommend the enactment of any additional legislative controls along these lines.**

10.5 An additional reason is that our proposals target surveillance whenever it is conducted by a "sense-enhancing, transmitting or recording device". This would encompass not only the comparatively specialised apparatus regulated by the Telecommunication Ordinance but also ordinary items such as tape recorders and binoculars. It is plainly unrealistic to endeavour to impose a licensing regime in respect of such items.

[1] South China Morning Post, 21 October 1995.

Licensing of private investigators

Private investigators: the United States experience

10.6 The regulation of surveillance requires a consideration of the nature of those who carry it out. Surveillance may be undertaken in the furtherance of specific public interests and we have proposed specific statutory tests for these. It is relevant to consider the activities of a sector whose work will often entail surveillance activities, namely private investigators. Unlike such public investigative bodies as the police, or the Independent Commission Against Corruption, however, there is comparatively little discussion of the role of private investigators in Hong Kong. Furthermore, they are not subject to institutionalised disciplinary regimes as apply to officers in law enforcement agencies. Accordingly, we have examined studies elsewhere. In their survey of United States private investigators,[2] Sam Brown and Gina Graham Scott point out that private investigator is in the business of gathering and selling personal information. Much of this will be obtained by covert means. The authors identify the following areas as comprising the main areas of the private investigator' s business in the United States:

- ***Family law***: Like the present Hong Kong law, many states in the United States have a fault-based system of divorce. Partners are therefore more disposed to seek verification of adultery, as it will facilitate their escaping the marriage and/or improve their bargaining position regarding the settlement. Another area is locate-and-recover operations concerning children kidnapped by one of their parents.

- ***Personal injury/workers compensation***: "Life style verifications" involve testing the claims of victims about the extent of injuries suffered and disabilities sustained. For example, a woman claimed a recent operation had left her nearly paralysed and mainly restricted to a wheelchair. Following medical doubts, visual surveillance was instituted and she was observed gardening and generally getting around unhindered.

- ***Prejudgment appraisals***: To determine whether a defendant is worth suing, an investigator may be hired to locate bank accounts, real estate, securities, and motor vehicles, or following judgement, the successful party may require this information.

- ***Financial background investigations***: Diligence advice is provided to companies contemplating entering into a contract with another company or individual, on the advisability of a loan, a merger, acquisition, franchise or other arrangement. One private investigator in this area referred to their role as "really acting like a super-sophisticated loan officer".

---

2 *Private Eyes,* Citadel (1991).

- ***Background investigations on political candidates/figures***: A political candidate may wish to unearth scandal, past or present. One investigator undertaking this work asserted that the activity resembled that of investigative journalism.

- ***Industrial espionage***: Obtaining proprietary information by covert means may facilitate significant profits. A company may quickly release products emulating that of its competitor, but at a significantly lower price. The lower price may result from the company not having had the high development costs in researching the new features. Instead, the innovations have been disclosed through industrial spying. Such spying may be an "inside job" involving an employee of the company.[3]

10.7 The activities of private investigators may overlap those of the police. On occasions, such as where drugs are discovered, private investigators will exercise the citizen's power of arrest and detain the person until a police officer has arrived. Prior to that, explains one investigator:

> *"We don't get the police involved in the beginning. You become a liaison or agent for the police or district attorney, and I don't want to have an agency relationship, because then, I'm encumbered with the Miranda rights requirement in interviewing people and all the other restrictions on search or seizure or privacy that relate to the police. For example, if I'm working with the police, I would have to tell suspects their rights during an interview, but I don't have to do that as a private investigator . . . But then, after the fact, if there is a crime involved, I call the police. If we found cocaine, I would tell the cops our discovery and ask them to make an arrest."* [4]

10.8 As indicated by this quote, the police are subject to additional legal and disciplinary controls not applicable to private investigators. That appropriate norms may not in place is indicated by the following comment of one investigator:

> *"There are really no black and white answers. In some ways, I'm all for personal privacy, and protecting the individual, which is why I won't take certain types of cases. But in other cases, I'm in favour of the public's right to know, and I think the right to get this information needs to be there. These are questions all private investigators can end up wrestling with, and ultimately I think it boils down to your own personal morality. . . I personally choose to turn down cases when I think I'm being asked to get information that's illegitimate. But then its up to each investigator to decide where to draw the line and*

---

3 Sam Brown and Gina Graham Scott, *Private Eyes,* (1991).

4 Brown and Scott, *op cit,* at 179.

whether he's going to draw it. And its not always easy to decide when to draw it. There are all these forces debating these issues, and even they can't always decide."[5]

10.9 In the United States many states impose a licensing regime on private investigators. In California, for example, 6,000 hours apprenticed to a licensed investigator is the minimum required.[6] This licensing requirement is supplemented by other controls. In California, regulation is exercised by the State Department of Consumer Affairs. In addition, professional groups within the field, like the California Association of Licensed Investigators, are working on increasing the professionalism and ethics in the field.

Private investigators in Hong Kong

10.10 In addition to local companies, several large international private investigation firms now operate in Hong Kong. Kroll Associates reports that much of its workload is in sweeping for the secret listening devices which are readily available in the territory.[7] In addition, presumably some or all of the above activities engaged in by United States companies are also undertaken here. Accordingly, the proposals contained in this paper will, if adopted, significantly impact on the activities of private investigators. In particular, if they involve surveillance or the interception of communications as defined in our proposed offences, it will be an offence to proceed without a warrant. It will be recalled that we have not proposed that only government bodies be entitled to apply for authorisation. On the contrary, we specifically envisage that private investigators may apply for a warrant where a relevant public exception is applicable, such as the prevention or detection of crime.

10.11 Unlike the position in the United States, private investigators in Hong Kong are not required to be licensed. **As to whether private investigators should be subject to a licensing requirement, we consider this issue to be beyond our terms of reference and we make no recommendation.**

---

5 *Ibid,* at 72.

6 *Ibid*, at 218.

7 *Sunday Morning Post,* 2 January 1994.

Chapter 11

Summary of recommendations

11.1 We do not recommend the creation of a general crime of trespass. *[paragraph 1.31]* Instead, we recommend a regulatory framework for the control of physical surveillance comprising three criminal offences along the following lines:

- entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein.*[paragraph 1.34]*

- placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier. *[paragraph 1.37]*

- placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant without the consent of the lawful occupier. *[paragraph 1.70]*

"Private premises" in this context means any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. In addition it should cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated; school premises; and commercial premises, aircraft, vessels and vehicles from which the public are excluded. *[paragraphs 1.36, 1.42 and 1.70]*

11.2 Communications should be safeguarded from interception or interference (including destruction or diversion) in the course of their transmission. *[paragraph 5.12]* It should be an offence:

- intentionally to intercept or interfere with (whether or not by means of a technical device) a communication transmitted by a distance communications system. Distance communications systems would encompass not only telecommunications system but also manual systems such as mail *[paragraphs 5.18 and 5.45]*

- intentionally to intercept or interfere with a "communication" by means of a technical device (whether or not the communication itself is mediated by means of a technical device), provided that the interception could not have been effected without the use of a device. *[paragraph 5.45]*

"Interference" for the purposes of these offences should include destruction or diversion. *[paragraph 5.45]*

11.3 A warrant should be required to authorise all surveillance or interception of communications falling within the scope of the proposed offences prohibiting these activities. *[paragraph 6.15]* All applications for warrants for surveillance or interception should be made to the High Court. *[paragraph 6.18]*

11.4 The sole grounds for issuing a warrant authorising intrusions should be **either** that it is for the purpose of preventing or detecting serious crime where:

- there is probable cause for suspicion of the target; and
- the information is not reasonably available by less intrusive means. *[paragraphs 6.41 and 6.48]*

or that it is for the purpose of security, defence, or international relations in respect of Hong Kong where:

- the intrusion is likely to be of substantial value in furthering these purposes; and
- the information cannot be reasonably obtained by other means. *[paragraph 6.50]*

"Serious crime" should mean either an offence punishable by at least 7 years imprisonment, or an offence punishable by at least 3 years imprisonment where there is an element of bribery or corruption. *[paragraph 6.36]*

"Security" should include safeguarding the stability of the local financial system. *[paragraph 6.54]*

11.5 A warrant should be issued for an initial period of 60 days and renewals should be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the original application) to continue to be necessary. *[paragraph 6.56]*

11.6 In circumstances where it is impractical 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. *[paragraph 6.20]*

11.7 Authorisation by warrant should be available to sanction intrusions by both public authorities and private companies. *[paragraph 6.21]*

11.8 Provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985 should be adopted, including the imposition of a requirement that the warrant-issuing authority ensure that adequate steps are taken to achieve compliance with the stipulations set out at paragraph 6.57. *[paragraph 6.60]* Surveillance and intercept materials should be inadmissible as evidence, regardless of their relevance.

[paragraph 6.68] This prohibition should extend to both authorised and unauthorised surveillance/ interception of communications. The prohibition should cover not only the fruits of surveillance but also details of methods used. *[paragraph 6.68]*

11.9 We reject as impractical the suggestion of imposing a requirement to notify an individual who has been subject to surveillance or interception of the cessation of that intrusion. *[paragraph 7.13]*

11.10 A Justice of Appeal should be appointed as the supervisory authority to review the issue of warrants authorising surveillance or the interception of communications. The applicable criteria should be those of judicial review. *[paragraph 8.27]*

11.11 The supervisory authority should be empowered to:

- review cases at the request of an aggrieved individual; *[paragraph 8.29]* and
- examine whether the warrant was properly issued and whether its terms have been complied with. *[paragraph 8.30]*

11.12 The supervisory authority should furnish annually a confidential report to the Governor and a public report to the Legislative Council. There should be a statutory requirement that the following matters be covered in both reports:

- the number of warrants authorised
- their average length and their extensions
- the classes of location of the surveillance i.e. domestic, business etc.
- the type of surveillance device used
- the number of persons arrested and convicted as a result of the surveillance or interception *[paragraph 8.34]*

11.13 Compensation should be payable for unauthorised intrusions. In addition to damages for actual loss suffered, in line with the Personal Data (Privacy) Ordinance, there should be compensation for injured feelings. Punitive damages should be available. *[paragraph 8.40]* We do not consider that a separate complaints tribunal will be required to supplement the role of the supervisory authority. *[paragraph 8.42]*

11.14 We do not recommend the licensing of surveillance equipment. *[paragraph 10.4]* We consider the question of the licensing of private detectives beyond our terms of reference and make no recommendation on this option. *[paragraph 10.11]*

Annexure

Breach of confidence[1]

Introduction

1 The consultation paper focuses on a comprehensive statutory scheme for the regulation of surveillance and prescribes a procedure for obtaining authorisation to engage in surveillance. Failure to obtain proper authorisation is a criminal offence. The paper does not consider the question as to whether surveillance should, in addition, be treated as a civil wrong. In its report *Breach of Confidence*[2] the English Law Commission considered the role of the duty of confidence in protecting improperly obtained information. The Commission noted that "it is a glaring inadequacy of the present law that ... the confidentiality of information improperly obtained, rather than confidentially entrusted by one person to another, may be unprotected." The Commission recommended that this situation be redressed by *treating* improperly obtained information as being impressed by a duty of confidence. The Commission identified the following situations as ones where it is reasonable to impose the duty:

> "*(i) A person should owe an obligation of confidence in respect of information acquired in the following circumstances:*
>
> *(a) by unauthorised taking, handling or interfering with anything containing the information;*
>
> *(b) by unauthorised taking, handling or interfering with anything in which the matter containing the information is for the time being kept;*
>
> *(c) by unauthorised use or interference with a computer or similar device in which data is stored;*
>
> *(d) by violence, menace or deception;*
>
> *(e) while he is in a place where he has no authority to be;*
>
> *(f) by a device made or adapted solely or primarily for the purpose of surreptitious surveillance where the user*

---

1 Much of the text of this annexure was prepared by Professor Raymond Wacks, a member of the sub-committee. The members of the sub-committee are indebted to Professor Wacks for his contribution to this part of the consultation paper.

2 Law Commission Report No. 110 (Cmnd 8388)

would not without the use of the device have obtained the information;

(g) by any other device (excluding ordinary spectacles and hearing aids) where he would not without using it have obtained the information, provided that the person from whom the information is obtained was not or ought not reasonably to have been aware of the use of the device and ought not reasonably to have taken precautions to prevent the information being so acquired.

(ii) An obligation of confidence shall be imposed on a person who jointly participates in the acquisition of information if, though he did not use any of the improper means listed in paragraph (i) above, he personally acquired the information and he is, or ought to be, aware that the information was acquired by the use of any such improper means by his fellow participator.

(iii) An obligation of confidence should not arise in accordance with paragraph (i) above where the information has been obtained by a person in the course of the lawful exercise of an official function in regard to the security of the State or the prevention, investigation or prosecution of crime or by a person acting in pursuance of any statutory provision so far as the information has been disclosed or used for those purposes or for any purpose expressly or impliedly authorised by a statutory provision."[3]

2 The Law Commission explains that it would be beyond its terms of reference to deem unlawful the use of any surreptitious surveillance device, and such a measure would be additional.

3 Items (f) and (g) are most directly relevant to our terms of reference. The distinction is made between devices primarily designed for surveillance purposes, and those lacking that specific purpose but which may nonetheless be so used e.g. binoculars or tape recorders. In both cases, the Commission recommends that the duty of confidence apply, provided that the information would not have been acquired without the use of such a device. However, the recommendation accommodates the fact that only in the former situation should it be assumed that the person from whom the information is obtained is not aware of the device' s use. Professor Wacks has identified a difficulty of the clause is that it is potentially restrictive:

"by prescribing a catalogue of specific forms of conduct there is a danger, especially in an area which is constantly undergoing technological change, of new methods of intrusion developing which call

[3] The Law Commission No 110, at para 6.46.

for legislative adaptation. A preferable analysis (suggested by the Scottish Law Commission) is to refer in a general manner to the acquisition by illegal means or by means which would be regarded as improper by a reasonable man."[4]

4 Whichever formulation is adopted, also relevant is the public interest defence in breach of confidence cases. Under the Law Commission's proposals:

"It should be for the defendant to satisfy the court that there was a public interest involved in the relevant disclosure or use of the information."

5 On 12 March 1985 the Home Secretary announced the Government's intention to legislate:

"*The Commission recommends that people who obtain information by 'improper means' - which includes the use of surveillance devices, as the Hon Gentleman knows - would be subject to an obligation not to use or disclose information. If they did so, they would be civilly liable to an action for breach of confidence. That approach has, I believe, the considerable advantage of concentrating on the real mischief -that is, the use to which information obtained is put. It provides the victim with a direct means of redress. I am able to announce today that the Government intends to introduce legislation based on the Law Commission's proposals. This will offer people an important and wholly new safeguard in an area of legitimate concern."*[5]

6 By 1990 legislation had still not been introduced and the Calcutt Committee declined to generally endorse the Commission's proposals, without adverting to this specific recommendation. That Committee's terms of reference were limited to "activities of the press". But other commentators have continued to urge the adoption of the draft clause quoted above. James Michael reviewed the disparate recommendations of the Younger Committee (1972), Law Commission, and the Calcutt Committee. The Younger Committee (whose terms of reference were restricted to the private sector) included a recommendation that it be a civil wrong "to disclose or otherwise use information which the discloser knows, or in all the circumstances ought to have known, was obtained by illegal means." James Michael concluded that:

"of the three proposals, the Law Commission's draft bill was the most carefully thought out [it represented 8 years of work] and the Government should not need a nudge from Sir David Calcutt to carry out the undertaking given by Leon Brittan when he was Home Secretary to legislate on the basis of it."[6]

---

4 Raymond Wacks, *Personal Information,* at p 263.

5 Quoted by James Michael in New Law Journal, May 4 1990 p 635.

6 Solicitor Journal, 31 July 1992 p 744.

7 Similarly, Patrick Milmo wondered:

> "*why the current demand for legislation to counter press intrusion on privacy cannot be met by [the Law Commission's draft] Bill rather than the vaguely formulated and controversial new law of privacy proposed by the Lord Chancellor.*"[7]

Recent developments in the law of confidence

8 The difficult question is whether, a third party, C, who intercepts a communication between A and B is liable to either A or B for breach of confidence. Where confidential information is acquired by the use of 'reprehensible means' (electronic surveillance, spying, and other forms of intrusive conduct), the authorities suggest the third party is not liable when he uses it. The apparent explanation for this 'glaring inadequacy'[8] (which means that if confidential information is obtained by improper means, it receives less protection by the law than if it were confided to a party who was under an obligation not to use or disclose it) is the absence of a relationship of confidence between the party who wishes to keep the information confidential, on the one hand, and another party, on the other.

9 But this may be a difficult position to defend. Thus, it has been argued[9] that in these circumstances the defendant, since he knew that the information was confidential (why else would he be surreptitiously obtaining it?), is under an imputed duty no different from that which applies to the ordinary recipient of confidential information.

10 Some breach of confidence cases lend support to the view that protection is not confined to consensual disclosures of confidential information. In *Lord Ashburton v Pape*,[10] the Court of Appeal, in a decision which involved the breach of confidence by a solicitor's clerk, referred to its power to enjoin the publication of information 'improperly or surreptitiously obtained'. More significantly, the Supreme Court of Queensland, in *Franklin v Giddens*[11] allowed an action for breach of confidence where the defendant had, in the absence of any confidential relationship, stolen genetic information in the form of cuttings from the plaintiff's unique strain of cross-bred nectarines. Dunn J said:[12]

> *"I find myself quite unable to accept that a thief who steals a trade secret, with the intention of using it in commercial competition with its*

---

7 New Law Journal, November 19 1993 p 1647.

8 Law Commission Report (note 1 above), paras 5.5 and 6.28. See generally Raymond Wacks. *Privacy and Press Freedom* (London: Blackstone Press, 1995), Chapters 3 and 5.

9 G Jones, 'Restitution of Benefits Obtained in Breach of Another's Confidence' (1970) 86 LQR 463.

10 [1913] 2 Ch 469, 475; approved in *Commonwealth of Australia v John Fairfax & Sons Ltd* (1980) 147 CLR 39, 50.

11 [1978] 1 Qd R 72.

12 *Ibid, 80.*

owner, to the detriment of the latter, and so uses it, is less unconscionable than a traitorous servant."

11 A persuasive case in support of the contention that the eavesdropper may be caught by the action for breach of confidence is the important decision in *Francome v Mirror Group Newspapers Ltd*[13] where the Court of Appeal granted an injunction to restrain the defendants from using information that had been obtained (by parties unknown) through the use of radio-telephony. The case conflicts with the judgment in *Malone v Commissioner of Police of the Metropolis (No 2)*[14] in which Sir Robert Megarry VC declined to make a declaration that telephone-tapping by the police was a breach of the victim's right of confidentiality in the conversations. In his view, an individual who divulges confidential information cannot complain when someone within earshot overhears his conversation. In the case of telephone conversations:

"The speaker is taking such risks of being overheard as are inherent in the system ... In addition so much publicity in recent years has been given to instances (real or fictional) of the deliberate tapping of telephones that it is difficult to envisage telephone users who are genuinely unaware of this possibility. No doubt a person who uses a telephone to give confidential information to another may do so in such a way as to impose an obligation of confidence on that other : but I do not see how it could be said that any such obligation is imposed on those who overhear the conversation, whether by means of tapping or otherwise."[15]

12 He was in no doubt that ' a person who utters confidential information must accept the risk of any unknown over-hearing that is inherent in the circumstances of the communication' .[16] Relying on this dictum, the defendants in *Francome* argued that the plaintiffs had no cause of action against them or the eavesdroppers for breach of an obligation of confidence. The Court of Appeal rejected this contention on the ground that in *Malone* the court was expressly concerned only with telephone-tapping effected by the police for the prevention, detection and discovery of crime and criminals. Fox LJ distinguished the two forms of intrusion in the following terms:

"Illegal tapping by private persons is quite another matter since it must be questionable whether the user of a telephone can be regarded as accepting the risk of that in the same way as, for example, he accepts the risk that his conversations may be overheard in consequence of the accidents and imperfections of the telephone system itself."[17]

---

13 [1984] 1 WLR 892.
14 [1979] 2 All ER 620.
15 *Ibid*, 376.
16 *Ibid*, 376.
17 [1984] 1 WLR 892, 900.

13 In other words a telephone user' s ' reasonable expectation of privacy' may be vindicated when the eavesdropper turns out to be a private individual, but not when it is the police acting under lawful authority. And it has been suggested that this judgment suffers from a ' fundamental misconception' :

> *"That because equity acts in personam it responds to some personal dealing between the parties so that the eavesdropper is in a quite different case to the confidant. But what the maxim indicates is that equity responds to unconscionable conduct by the defendant; this may but need not flow from any consensual dealing with the plaintiff. Accordingly, it requires no great effort, no straining of principle to restrain the activities of the eavesdropper."*[18]

14 The absence of a relationship between the parties has not inhibited the Hong Kong courts from imposing liability for breach of confidence. In *Koo and Chiu v Lam*,[19] the Hong Kong Court of Appeal recently held that a medical researcher was under a duty of confidence in respect of a questionnaire that had been prepared by a ' rival' research team and which, by the appellant' s admission, he had used formulating his own questionnaire. It is unfortunate that there is no clear evidence as to how the appellant obtained access to the respondents' questionnaire. Penlington JA, commenting upon the trial judge' s finding that the appellant had obtained the information ' surreptitiously' , remarked:

> *"He did somehow come into possession of the document, and he must have known it was confidential because of the amount of work which had gone into its preparation. It had not been given to him by the persons whose information it was and again he must have realised he was not entitled to use it."* [20]

15 This dictum takes the law considerably further than both *Franklin* and *Francome* for in those decisions the ' surreptitious taker' acted contrary to law (theft and an offence contrary to the UK Wireless Telegraphy Act 1949, respectively). In *Koo,* Penlington JA emphasised that the finding of ' surreptitious obtaining' did not extend as far as theft which, he said ' cannot be supported by the evidence' .[21] But if surreptitious taking extends to the mere fact that the appellant ' did somehow come into possession' of the questionnaire with the knowledge that it was confidential, the Hong Kong Court of Appeal appears (by accident or design) to have grasped the nettle and embraced the notion of receipt-based liability, albeit under cover of surreptitiousness rather than unconscionability.

16 Some caution is, however, required. First, the actual finding, at first instance, that the information was imparted in circumstances imposing an obligation of

---

18 Meagher *et al* (note 28 above), p 827. See Wacks, *Personal Information*, pp 256-9.
19 Civil Transcript No 116 (1992).
20 *Ibid*, 30.
21 *Ibid*, 29.

confidence (the second *Saltman* limb) was not challenged upon appeal.[22] Secondly the rival teams of researchers worked at the same university which implied a 'course of dealing' between the parties during which the appellant arguably became aware that the questionnaire was confidential. This could, to some extent, approximate to a relationship of confidence on orthodox principles.

17 The decision is plainly not one of a stranger stumbling across a diary in the street. Nevertheless, assuming it is correct, the judgement demonstrates the utility of the breach of confidence action where the strict requirement of a prior relationship is relaxed. It does not, however, remove all the obstacles in the path of the protection of 'privacy', for the finding that the appellant knew that the information contained in the questionnaire was confidential was derived less from the nature of the information than from his personal experience, and the limited relationship between the parties.

18 Nevertheless, to catch the eavesdropper, the Younger Committee considered legislation necessary:[23]

> *"We think that the damaging disclosure or other damaging use of information acquired by any unlawful act, with knowledge of how it was acquired, is an objectionable practice against which the law should afford protection. We recommend therefore that it should be a civil wrong, actionable at the suit of anyone who has suffered damage thereby, to disclose or otherwise use information which the discloser knows, or in all the circumstances ought to have known, was obtained by illegal means. It would be necessary to provide defences to cover situations where the disclosure of the information was in the public interest or was made in privileged circumstances. We envisage that the kinds of remedy available for this civil wrong would be similar to those appropriate to an action for breach of confidence."*

19 One difficulty with this approach is that the Younger Committee rejected the introduction of an action for unwanted publicity; the only remedies considered necessary in cases of 'public disclosure' were the action for breach of confidence and this one which will only assist the plaintiff where the information was acquired *unlawfully*. This means that where, say, a journalist obtains personal information *lawfully*, the plaintiff will have no remedy. But should unlawful means be employed, an action may lie, subject to the proposed defence of 'public interest'. In other words, in the view of the Younger Committee, the only circumstances under which a civil action would lie where there has been disclosure of personal information are where the means used to obtain the information were unlawful. And this confuses the interests in issue in 'intrusion' with those that arise in 'disclosure'. Since the availability of remedy is, prima facie, made dependent upon the use of illegal means, the question of whether there has been an intrusion becomes a crucial criterion in determining whether the plaintiff has a remedy at all. This factor ought *not* to be of primary importance in

---

22 One is bound to ask 'why not?' The decision of the trial judge represents a significant divergence from existing authority.

23 *Younger*, Para 632.

cases of disclosure. Equally, unlawful means ought not to be permitted merely because the eventual disclosure is justified. The two questions should be kept separate.

20 The Law Commission recognise that there is an important distinction between the imposition of an obligation of confidence in the normal case, and in the case of improper acquisition, when they state:[24]

> *"There is undoubtedly a considerable difference in nature between on the one hand the obligation imposed on a person for breaking an undertaking to another to keep information confidential and, on the other, an obligation imposed on a person as a result of his having used improper means to gain information which may, indeed, be so secret that the plaintiff has never entrusted it to anyone, not even in confidence. Nevertheless, we believe that it is possible to encompass both forms of behaviour within the framework of our new statutory tort."*

21 They conclude that the common feature in both cases is that the receiver of information is in a position where it is *reasonable* to impose a duty of confidence upon him. They therefore propose a number of situations[25] in which the acquirer of information should, by virtue of the manner in which he has acquired it, be treated as being subject to an obligation of confidence in respect of such information acquired in the following circumstances:

(a) by unauthorized taking, handling, or interfering with anything containing the information;

(b) by unauthorized taking, handling, or interfering with anything in which the matter containing the information is for the time being kept;

(c) by unauthorized use of or interference with a computer or similar device in which data are stored;

(d) by violence, menace, or deception;

(e) while he is in a place where has no authority to be;

(f) by a device made or adapted solely or primarily for the purpose of surreptitious surveillance where the user would not without its use have obtained the information;

(g) by any other device (excluding spectacles and hearing aids) where he would not, without using it, have obtained the information, provided that the person

---

24 Law Commission Report, Para 6.30.

25 *Ibid*, Para 6.46.

from whom the information is obtained was not or ought not reasonably to have been aware of the use of the device and ought not reasonably to have taken precautions to prevent the information being so acquired.

22 This approach is potentially restrictive: by prescribing a catalogue of specific forms of conduct there is a danger, especially in an area which is constantly undergoing technological change, of new methods of intrusion developing which call for legislative adaptation. A preferable analysis (suggested by the Scottish Law Commission)[26] is to refer in a general manner to the acquisition by illegal means or by means which would be regarded as improper by a reasonable person. This has the advantage of anticipating advances in electronic surveillance technology. The English Law Commission would impose automatic liability ' without qualification'[27] for the use of confidential information upon a person who obtains such information with the assistance of a device which is ' clearly designed or adapted solely or primarily for the surreptitious surveillance of persons, their activities, communications or property' .[28]

23 They draw a distinction between such devices and those, such as binoculars or tape recorders, which are not in themselves designed primarily for that purpose, although they are capable of being so used. In the case of the latter, liability for the subsequent use or disclosure of the information should arise only if the subject was not or ought not reasonably to have been aware of the use of the device and failed to take precautions to prevent its acquisition.[29] This would seem to be a sensible distinction.

24 The Scottish Law Commission would impose an automatic obligation on a person not to use or disclose *any* information so acquired ' however trivial it may seem to an outsider' .[30] The obligation is therefore not dependent on the nature of the information acquired; it is not restricted (though, in practice, will normally relate) to confidential information. While consistent with the general concern to prevent intrusive activities (and not merely their consequences), this proposal again demonstrates the different objectives of the control of intrusion, on the one hand, and the protection against the *misuse* of personal information, on the other. The former extends beyond (but may accommodate) the present concern with confidential information and, *a fortiori*, personal information, and is, of course, in any event, more satisfactorily dealt with by the criminal law or by administrative control.

25 No obligation of confidence should be imposed upon a ' surreptitious taker' by virtue only that he used illicit means to obtain the information. Liability should always rest upon general principles of unconscionability; the fact that improper means were necessary to acquire the information is persuasive in deciding whether the defendant had constructive knowledge, but is not an inexorable rule of law.

---

26 Scottish Law Commission, *Breach of Confidence* (Scot Law Com No 90, 1984), Paras 4.36-41.
27 Law Commission Report, Para 6.35.
28 *Ibid.*
29 *Ibid,* Para 6.38.
30 Scottish Law Commission, Para 4.38.

26 To what extent, if at all, is the fact of intrusion punished by the action for breach of confidence? As in the American jurisprudence, the English case law suggests a tendency to confuse intrusion and disclosure. In *Malone*, the plaintiff's telephone had been tapped by the Post Office under a warrant signed by the Secretary of State; Malone being under suspicion of handling stolen goods. In the course of his judgment, Sir Robert Megarry VC, having adverted to Lord Denning's 'just cause or excuse' formulation for the public interest defence,[31] remarks that 'the question is ... whether there is just cause or excuse for the tapping and for the use made of the material obtained by the tapping'.[32] This is to confuse the two issues.

27 In *Francome*, the Court of Appeal upheld the granting of an interlocutory injunction to prevent the defendants from disclosing information concerning the jockey Peter Francome which had been obtained by telephone tapping. An important distinction between this decision and *Malone* is that in the latter the defendant was both the intruder and the potential discloser, whilst in *Francome* the intruders were not a party to the proceedings. Thus, maintaining the rigid and logical distinction suggested above, the only pertinent question here is whether the *Daily Mirror* received the information subject to an obligation not to disclose it to others. Again, the fact of the tapping does figure in this assessment, but only in so far as it might determine what reasonably constitutes unconscionable behaviour.

28 The analysis of Sir John Donaldson MR is in this respect correct. That he realised that intrusion was not in issue is clear from his comment that the question at trial 'is likely to be whether the defendants can make any, and if so what, use of the fruits of [the illegal tapping]'.[33]

Reforming the law

29 In its *Report on Breach of Confidence*, the Law Commission advocated the creation of a statutory tort of breach of confidence. Having concluded that, under the existing principles of the equitable action for breach of confidence,[34] the plaintiff has no protection where information is surreptitiously taken from him (as opposed to his having imparted it to another in circumstances imposing an obligation of confidentiality[35]), the Commission proposed that if information were so acquired, the 'surreptitious taker' and any person obtaining the information from him, with knowledge, was under an obligation of confidence by virtue solely of that surreptitious taking.[36]

30 This approach conflates disclosure and intrusion; the fact of intrusion is the basis upon which disclosure is to be prevented or compensated. And the Law Commission

---

31 See *Fraser v Evans* [1969] 1 QB 349, 362.

32 [1979] Ch 345, 377.

33 [1984] 1 WLR 892, 895.

34 See *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413.

35 In Para 5.5 of the Report, the Law Commission states: 'It is a glaring inadequacy of the present law that ... the confidentiality of information improperly obtained, rather than confidentially entrusted by one person to another, may be unprotected'. The reasoning by which the Commission reaches this conclusion is set out in paras 4.7-4.10.

36 This proposal is embodied in clause 5 of the draft bill (*ibid*, Appendix A).

propose no separate sanctions against intrusion itself.[37] In clause 14(1)(b) of their draft bill, the Commission define recoverable damages to include those in respect of ' any mental distress, and any mental or physical harm resulting from such distress' in consequence of the defendant's breach of confidence. This explicit restriction of those damages to distress suffered in ' consequence of the breach'[38] suggests that, along with the narrowness of the Commission's terms of reference mentioned above, it is highly unlikely that the Commission envisaged an enhancement of these damages by virtue of additional distress caused by the intrusion.[39] The Law Commission Report proposed no sanction for the act of intrusion per se, preferring, as is logically consistent with its terms of reference, to use the intrusion as a springboard from which to attach an obligation of confidence to prevent or compensate disclosure.

31 In its report, the Calcutt Committee[40] recommended that three forms of physical intrusion should be criminal offences, namely:

(a) Entering private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication;

(b) Placing a surveillance device on private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication;

(c) Taking a photograph, or recording the voice, of an individual who is on private property, without his consent, with a view to its publication with intent that the individual shall be identifiable.[41]

It proposed a public interest type defence to these offences.[42]

32 Just as the Law Commission concentrates exclusively on disclosure, so the Calcutt Committee directs its legislative recommendations at intrusion, leaving disclosure to the regulation of a newly formed Press Complaints Commission.[43] The prospect of confusion between the two issues is thus obviated.

---

37 Though this may be readily explained by reference to the terms of reference of the Commission' s enquiry. The relevant term asks the Commission to : ' consider and advise what remedies, if any, should be provided for persons ... who have suffered loss or damage *in consequence of the disclosure or use of information unlawfully obtained* and in what circumstances such remedies should be available' . (*ibid*, Para 1.1)

38 Clause 14(1)(b) of the draft bill.

39 This view is supported by para 6.106 of the Report where the Commission confine its analysis to ' mental distress' suffered *as a result of the breach of confidence.*

40 Calcutt Report.

41 *Ibid*, para 6.33.

42 *Ibid,* para 6.35. The defences are : ' (a) for the purpose of preventing, detecting or exposing the commission of any crime, or other seriously anti-social conduct; (b) for the protection of public health or safety; or (c) under any lawful authority' . This approach was again proposed by the Calcutt in his Review, with minor alterations (paras 7.1-7.26).

43 *Ibid*, paras 15.1-15.31.

33 The National Heritage Committee[44] recommend the introduction of a Protection of Privacy Bill, one part of which concerns what the Committee call ' the main civil offence' , namely infringement of privacy[45] and it is clear from the definition of that offence that liability attaches to both ' obtaining and/or publishing' personal information.[46] Here, however, intrusion and disclosure are entirely separated, each, independently, giving rise to a cause of action. But, again, it is to be regretted that a public interest defence is proposed to apply both to acts of publication and to the *obtaining* of the personal information.[47] The bill includes provisions along the lines of the Calcutt Report for the introduction of criminal sanctions against certain intrusive techniques.[48]

---

44 National Heritage Committee.

45 *Ibid*, para 48.

46 *Ibid*.

47 *Ibid*, and see para 55.

48 *Ibid,* para 52