ARTICLES

REMEDIES AGAINST TELEPHONE TAPPING BY THE GOVERNMENT

*Ng Hon Wah**

Telephone tapping, a measure adopted by law enforcement agencies for the prevention and detection of crime, is carried out under section 33 of the Telecommunications Ordinance. However, the section does not pass the forseeability test required for it to be regarded as "law". The present practice of telephone tapping violates the right to privacy and to freedom of expression guaranteed by the Basic Law. The Personal Data (Privacy) Ordinance, which may be invoked by persons suspecting their telephones to have been tapped, has limitations. These people stand a better chance by relying on the Hong Kong Bill of Rights Ordinance. Accordingly, to avoid the courts being landed with the invidious task of either rendering the rights in question a nullity or denying law enforcement agencies a necessary tool, the Hong Kong Special Administrative Region (HKSAR) Government should take immediate action to enact legislation along the lines recommended by the Law Reform Commission in 1996.

Introduction

In contrast to the massive demonstration against the National Security (Legislative Provisions) Bill 2003 for its possible restriction on the rights and freedoms enjoyed in Hong Kong, human rights activists have, over the years, shown little concern about an existing enactment which interferes with the right to the freedom and privacy of communication.

Telephone tapping, probably resorted to daily by law enforcement agencies, is governed under section 33 of the Telecommunications Ordinance (Cap 106), which provides that:

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

* Doctor of Legal Science (SJD) student, Faculty of Law, University of Hong Kong. I wish to express my sincere thanks to my supervisor, Carole Petersen, for her encouragement and comments on the draft of this article.

telecommunication, shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order."[1]

Before 1 July 1997, interceptions of communications were authorised by the Governor personally and "only when the public interest so require(d) and only in cases involving the prevention or detection of serious crime, including corruption, or in the interests of the security of Hong Kong".[2] After the reversion of sovereignty, the power has been delegated to the Chief Secretary for Administration.[3] The Government has not explained which crimes are regarded as serious. The damaging disclosure of official secrets, an offence attracting a fine of $500,000 and imprisonment for two years,[4] can conceivably qualify as one. Even if it does not, telephone tapping aimed at tracking down moles will fall within the broad expression of "in the interests of the security of Hong Kong".

The public has no idea how frequently the power is exercised. The Government has steadfastly refused to disclose to the Legislative Council (LegCo) the number of cases involved.[5] The author's enquiry in early 2003 on the ranks of authorised public officers and other related matters has drawn a complete blank, with the Security Bureau replying that "for operational and security reasons, I am afraid we are unable to comment further on the work relating to interception of communication as doing so would risk compromising the operation of our law enforcement agencies".[6] The fact that the Bureau did not even repeat information already available in the public domain (eg that the personal consent of the Chief Executive or the Chief Secretary for Administration is required) gives rise to suspicion that the Government may have relaxed its internal guidelines.

1 References to "the Governor" have not been amended by any of the Adaptation of Law Ordinances enacted after the reversion of sovereignty. Pursuant to s 2A(3) of the Interpretation and General Clause Ordinance (Cap 1), read in conjunction with item 11 in Sch 8 thereto, the term "Governor" shall be interpreted as referring to "the Chief Executive of the Hong Kong Special Administrative Region".

2 Secretary for Security's reply to a question asked by the Hon Gilbert Leung. *See* Hong Kong Legislative Council Official Record of Proceedings for meeting held on 11 Nov 1992, p 634. The reply was quoted in Law Reform Commission of Hong Kong, Report on *Privacy: Regulating the Interception of Communications* (Hong Kong: Government Printer, Dec 1996) para 2.23. The Government's internal arrangement that authorisation must be given by the Governor personally appeared to continue up to 1997. *See* para 4 of the minutes of the joint meeting of the LegCo Panel on Information Policy and LegCo Panel on Security held on 18 Feb 1997 (LegCo Paper No. CB(2)1635/96-97), which records that "(a)ny interceptions had to be authorised by the Governor"

3 Secretary for Security's reply to a question asked by the Hon James To. *See* Hong Kong (China) Legislative Council Official Record of Proceedings for meeting held on 10 Nov 1999, p 1068. The Secretary for Security pointed out that interception "can be done only after the Chief Executive or the Chief Secretary for Administration has given their personal consent".

4 S 25(1)(a), Official Secrets Ordinance (Cap 521).

5 *See* Hong Kong (China) Legislative Council Official Record of Proceedings for meeting held on 30 Sept 1998, pp 1928–1931, in particular the comment made by the Hon James To, p 1929.

6 Security Bureau's e-mail dated 26 Feb 2003.

This paper recounts the efforts to introduce specific legislation to regulate the interception of communications, outlines the basis for considering section 33 to be unconstitutional, examines the possibility of invoking the Personal Data (Privacy) Ordinance (PDPO) (Cap 486) and the Hong Kong Bill of Rights Ordinance (HKBORO) (Cap 383) to seek remedies, and concludes that a responsible government must act quickly to enact the necessary legislation.

Efforts to Introduce Legislation

Section 33 came under the scrutiny of the Law Reform Commission (LRC) shortly before the reversion of sovereignty.[7] Taking into account the jurisprudence of the European Court of Human Rights (ECHR), the LRC opined that the section "may not reflect the provisions of the ICCPR and Basic Law" which protect the right to privacy.[8] It recommended a regulatory framework, under which judicial warrants are required for interceptions of communications.[9] Following the report, the Government published a White Bill on Interception of Communications for public consultation in February 1997.[10] The Bill was left on ice on the ground that the 14 submissions received raised "significant technical and policy issues" and that the legislative proposal would not receive sufficient support in the then LegCo.[11]

The assessment of LegCo's support proved to be wrong. The Interception of Communications Ordinance, based on a Member's Bill moved by the Hon James To to force the Government's hands, was passed by the Council on 27 June 1997.[12] Section 1(2) therein provides for the Governor to appoint the commencement date. Despite repeated pressure from some legislators,[13] no such date has been appointed. The Government argues that this ordinance includes provisions which would pose enormous difficulties to

7 Law Reform Commission (LRC). *See* Report on *Privacy* (n 2 above).

8 *Ibid.*, para 2.21. "ICCPR" stands for International Covenant on Civil and Political Rights.

9 *Ibid.*, Ch 6.

10 Security Branch, Consultation Paper on *Interception on Communications Bill* (Feb 1997). The White Bill included the LRC's recommendation for a judicial warrant system but not some of the related recommendations. *See* minutes of joint meeting of LegCo Panel on Information Policy and LegCo Panel on Security held on 7 Mar 1997 (LegCo Paper No. CB(2)1857/96-97), para 6.

11 Letter dated 5 May 1997 from Governor Chris Patten to Hon Dr Leong Che-hung, Chairman of LegCo's House Committee (copy obtained from Legislative Council Library).

12 Ordinance No. 109 of 1997, Legal Supplement No. 1 to the Hong Kong Government Gazette Extraordinary, 30 June 1997, at pp A3903-A3931.

13 *See* questions and answers in LegCo meetings (nn 3 and 5 above).

law enforcement agencies in crime prevention and detection.[14] It claims to have been undertaking a comprehensive review on the whole issue in the light of overseas practices.[15]

Is Section 33 Constitutional?

Constitutional Framework

The HKBORO incorporates the International Covenant on Civil and Political Rights (ICCPR), which acquires constitutional status vide Article 39 of the Basic Law (BL). The BL also contains specific provisions to guarantee the individuals' rights, including the right to freedom and privacy of communication under Article 30. General comments issued by the United Nations Human Rights Committee (HRC) and jurisprudence of the HRC and ECHR are of persuasive value in interpreting ICCPR.[16]

Relevant Provisions in International Human Rights Instruments

Numerous cases before the ECHR, discussed below, have firmly established telephone tapping to be an intrusion of privacy. In Hong Kong, ICCPR Article 17, which has been incorporated as Article 14 of the Bill of Rights (BOR) within the HKBORO, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy". In its General Comment 16 on Article 17, the HRC explained the expression "arbitrary or unlawful interference" as follows:

> "The term 'unlawful' means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[17]
>
> "In the Committee's view the expression 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[18]

14 *See*, for example, Secretary for Security's replies in Hong Kong (China) Legislative Council Official Record of Proceedings for meeting held on 10 Nov 1999, pp 1066–1073.

15 *Ibid.*

16 *See* Johannes Chan, "Hong Kong Bill of Rights Ordinance (Cap 383) – Introduction" in *Annotations to the Hong Kong Bill of Rights Ordinance* (Butterworths Asia, 1999), pp 1–8, at pp 4–6.

17 CCPR General Comment 16, 4 Aug 1988. Available at http://www.unhchr.ch/tbs/doc.nsf/ (last visited on 22 Feb 2003), para 3.

18 *Ibid.*, para 4.

> "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 authorized interference must be made only by the authority designated under the law, and on a case-by-case basis."[19]

In the Convention for the Protection of Human Rights and Fundamental Freedoms (EHRC), the right to "private and family life" is protected by Article 8, which, like ICCPR Article 17, requires that any interference with the right must be in accordance with the law. It also lists the legitimate objectives for which interference may be justified.[20]

Telephone tapping can also be a restriction of the freedom of expression. Under ICCPR Article 19 (BOR Article 16), the right to freedom of expression "shall include freedom to seek, receive and impart information and ideas of all kinds". By extension, it must include the right *not* to impart information or ideas to anyone other than the intended recipients. Big Brother's eavesdropping would have a chilling effect on communication. In particular, the possibility of informants' identities being ascertained by the power-that-be would inhibit some of them from speaking to reporters about public affairs. ICCPR Article 19(3) provides that restrictions "shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (*ordre public*), or of public health or morals". Similarly, EHRC Article 10 requires that any restriction of freedom of expression be prescribed by law. It is more specific than ICCPR Article 19 as regards the grounds on which restrictions may be justified.[21]

International Jurisprudence

The author's research has not unearthed any complaint about telephone tapping being considered by the HRC. However, the ECHR offers a wealth of jurisprudence on the subject. In the leading case of *Malone v United Kingdom*,[22]

19 *Ibid.*, para 8.

20 EHRC Art 8(2) reads "There shall be no interference 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."

21 EHRC Art 10(2) reads "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

22 (1985) 7 EHRR 14, [1984] ECHR 8691/79.

the applicant, who was acquitted in the UK of charges relating to dishonest handling of stolen goods, complained to the ECHR that his incoming letters had been intercepted and his telephone tapped by the police, in violation of his right to privacy under EHRC Article 8. The UK government admitted that one single conversation revealed in the criminal trial had been intercepted on behalf of the police pursuant to a warrant issued by the Secretary for State.[23] The legal basis for such a warrant was section 80 of the Police Office Act 1969.[24] The practice, as summarised in a UK Government's White Paper, was that:

> "Law enforcement agencies might request authority for the interception of communications for the purposes of 'detection of serious crime and the safeguarding of the security of the State'".[25]
>
> "In the case of warrants applied for by the police to assist them in the detection of crime, three conditions must be satisfied before a warrant will be issued: (a) the offence must be 'really serious'; (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 a conviction."[26]

It was common ground that interception of the telephone conversation in question amounted to interference with the right protected under Article 8.[27] On the question whether the interference was "in accordance with the law", the ECHR referred to its ruling in earlier cases that for any written or unwritten law to satisfy the requirement of "in accordance with the law", it must pass the tests of accessibility[28] and foreseeability.[29] The requirement of foreseeability varies according to context. In the context of interception of communications, the ECHR held:

> "The requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, *the law must be sufficiently clear in its terms to give citizens an adequate*

23 *Ibid.*, para 16.
24 *Ibid.*, para 29.
25 *Ibid.*, para 42.
26 *Ibid.*
27 *Ibid.*, para 64.
28 *Ibid.*, para 66. For a law to pass the accessibility test, "the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case".
29 *Ibid.*, para 66. "A norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."

> *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*".[30]

The ECHR noted that first, detailed procedures concerning interception of communications did exist in the UK; secondly, published statistics showed the number of warrants to be reasonably low; and thirdly, the public had been made aware of the arrangements and principles through various official reports and statements.[31] Its conclusion was nevertheless that:

> "On the evidence before the Court, 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 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. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking."[32]

Following the ECt's ruling that the law in England and Wales failed the foreseeability test, the UK Government enacted the Interception of Communications Act 1985, the objective of which "was to provide a clear statutory framework within which the interception of communications on public systems would be authorised and controlled in a manner commanding public confidence".[33]

The European cases on telephone tapping all dealt with it as interference with the right to privacy. In three of them, the applicants also alleged violation of freedom of expression. The ECHR, after finding violation of the right to privacy, did not consider it necessary to examine the other allegation.[34] No doubt, the *Malone* principle is equally applicable in considering an allegation of telephone tapping in the context of freedom of expression. Indeed, *Sunday Times v United Kingdom*,[35] where the ECHR developed the accessibility and foreseeability tests applied in *Malone*, was a case dealing with press freedom.

30 *Ibid.*, para 67. Emphasis added.
31 *Ibid.*, para 79.
32 *Ibid.*
33 *Halford v United Kingdom* (1997) 3 BHRC 31, para 21. The 1985 Act has now been replaced by the Regulation of Investigatory Powers Act 2000.
34 *Silver v United Kingdom* (1983) 5 EHRR 347, [1983] ECHR 5947/72, paras 106–107; *Schonenberger and Durmaz v Switzerland* (1989) 11 EHRR 202, [1988] ECHR 11386/85, para 31; *Halford v United Kingdom* (n 33 above), para 21.
35 (1980) 2 EHRR 245, [1979] ECHR 6538/74. The two tests were developed in para 49 therein.

Since even the UK law, with its relatively detailed operational procedure made known to the public, did not pass the foreseeability test, it is clear that section 33 of the Telecommunications Ordinance, with its loose reference to "the public interest so requires" and the cloak of secrecy surrounding its operation, falls a long way short of the requirement of providing the citizens with adequate indications as to the circumstances in which, and the conditions on which, the authorities may resort to telephone tapping. In Hong Kong, the test was applied by the Court of Final Appeal, in *Shum Kwok Sher v HKSAR*,[36] in relation to the common law offence of misconduct in public office. Holding the offence to pass the test, the court cited British and Canadian authorities for the view that the degree of precision required depended on the context and some laws in furtherance of valid social objectives had to be framed in general terms in order to cope with changing circumstances.[37] Mr Justice Bokhary PJ qualified that for the type of offences which limited fundamental rights such as free speech, "an exceptionally high degree of certainty of definition would be required".[38] While section 33 does not create an offence, it is a provision interfering with fundamental rights. Its terms – that interception may be ordered "whenever ... the public interest so requires" – are way below the "exceptionally high degree of certainty" required. One can see no practical difficulty in defining more precisely the circumstances in which interception may be permitted.

If Hong Kong courts are persuaded by the ECHR's case laws – and there appears to be no ground for distinguishing the situation in Europe from that in Hong Kong – it is more than likely that section 33 will not be regarded as "law" for the purpose of ICCPR Articles 17 and 19 (and BOR Articles 14 and 16). In the absence of any legal basis, telephone tapping will in all cases violate the Basic Law and HKBORO, regardless of whether the measure, in a particular case, is a necessary and proportionate response in the interests of crime prevention and detection or other legitimate objectives.

Hong Kong Cases on Telephone Tapping

In Hong Kong, the question of whether telephone tapping violates the BOR came before the higher courts in two cases. An issue in both *R v Cheung Kai Fai*[39] and *Re Thanat Phaktiphat*[40] was whether telephone conversations intercepted by foreign law enforcement agencies from telephones used overseas

36 Final Appeal No. 1 of 2002 (Criminal) (Court of Final Appeal, 10 July 2002), last accessed via Judiciary's website at http://legalref.judiciary.gov.hk on 5 Sept 2003.

37 *Ibid.*, paras 89–92, per Sir Anthony Mason NPJ.

38 *Ibid.*, para 3.

39 Criminal appeal No. 198 of 1992 (Court of Appeal, 22 Aug 1995), last accessed via Judiciary's website at http://legalref.judiciary.gov.hk on 27 May 2003.

40 Miscellaneous Proceedings No. 2904 of 1994 (High Court, 24 Nov 1994), last accessed via Judiciary's website at http://legalref.judiciary.gov.hk on 27 May 2003.

could be admitted as evidence against the speakers in criminal and extradition proceedings, respectively. The courts answered affirmatively in both cases. However, since the interception took place outside Hong Kong and section 33 was not involved, neither case throws any light on whether the section was consistent with the BOR.

Do the Laws in Hong Kong Provide Sufficient Protection Against Telephone Tapping?

BL Article 30 provides that "the freedom and privacy of communication of Hong Kong residents shall be protected by law". Apart from the HKBORO, what laws are there to protect citizens from telephone tapping?

No Criminal Sanctions Against the Government

Section 33 does not provide any protection against telephone tapping. By empowering the Chief Executive and authorised public officers to make orders for interception, it enables interception without making any unauthorised interception unlawful. The Telecommunications Ordinance provisions which can be invoked to prohibit unauthorised interceptions are sections 27,[41] 20,[42] 27A[43] and 24.[44] The sections do not bind the Government.[45] Nor, it appears, is there any other legislation or common law to make telephone tapping by the Government an offence.[46]

41 S 27 provides that "any person who damages, removes or interferes in any way whatsoever with a telecommunication installation with intent to ... (b) intercept or discover the contents of a message ..." shall be guilty of an offence. *See* para 2.5 of LRC's report (n 2 above).

42 S 20 makes it an offence for any person, without a licence, to "(a) establish or maintain any means of telecommunications; or (b) possess or use any apparatus for radiocommunications or any apparatus of any kind that generates and emits radio waves notwithstanding that the apparatus is not intended for radiocommunications". *See* the LRC's comments on the offence in paras 2.6–2.8 of its report (n 2 above). The reference to s 8 in LRC's para 2.6 should appropriately read "Sections 8 and 20".

43 S 27A provides that "any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer commits an offence". For discussion of the section, *see* paras 2.9–2.19 of the LRC's report (n 2 above).

44 Under s 24, "a telecommunications officer, or any person who, though not a telecommunications officer, has official duties in connection with a telecommunications service" commits an offence if he "... (c) ... wilfully intercepts or detains or delays any message; (d) otherwise than in pursuance of his duty or as directed by a court, copies any message or discloses any message or the purport of any message to any person other than the person to whom the message is addressed".

45 S 3 of the Telecommunications Ordinance provides that "save as otherwise expressly provided, this Ordinance does not bind the Crown ...". Pursuant to s 2A(3) of the Interpretation and General Clauses Ordinance read in conjunction with item 2 in Sch 8 therein, any reference to "the Crown" shall be construed as a reference to the Hong Kong Special Administrative Region (HKSAR) Government.

46 The author has not conducted the comprehensive research necessary to make a firmer statement on the subject. The LRC's report (n 2 above) does not mention any other applicable offence.

Insufficient Civil Remedies

As regards civil remedies, "there is no right of privacy at common law. Such protection for the privacy of individuals as there is at common law is inadequate in safeguarding the privacy of communications".[47] Certain torts, such as trespass of land and nuisance, can be invoked to address some acts which are incidental to telephone tapping. They, however, do not apply where telephone tapping is done in such a way that the victim being spied upon suffers merely emotional distress but not any physical harm or damage to property.[48]

Personal Data (Privacy) Ordinance (PDPO)

Subject to the inadequacies to be discussed below, the PDPO, which regulates the collection and use of personal data, may provide remedies against injudicious telephone tapping carried out by the Government or other persons. The PDPO embodies six internationally accepted data protection principles (DPP) developed by the Organisation for Economic Cooperation and Development (OECD).[49] DPP 1 provides that a data user[50] shall not collect more personal data than necessary for a lawful purpose related to his functions or activities[51] and shall collect by means that are lawful and fair in the circumstances.[52] DPP 2 requires a data user to take practicable steps to ensure the accuracy of personal data in his holding[53] and prohibits the keeping of personal data for longer than necessary.[54] DPP 3 prohibits the use of personal data, without the data subject's voluntary and express consent, for any purpose other than those related to the original purpose of collection.[55] DPP 4 requires that practicable steps be taken to ensure the security of personal data held by a data user.[56] DPP 5 requires a data user to maintain transparency as

47 *See* para 3.2 of LRC's report (n 2 above).

48 For discussions of the torts relevant to interception of communications and invasion of privacy, *see* Ch 3 "The legal protection of privacy of communications" in LRC's report (n 2 above); Ch 4 "Protection of privacy at common law" in Hong Kong Law Reform Commission's Sub-committee on Privacy, Consultation Paper on *Civil Liability for Invasion of Privacy*, (Hong Kong: Printing Department, Aug 1999); and Ch 4 "Data privacy and the common law" in Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law – Territorial Regulation in a Borderless World* (Hong Kong, Singapore and Malaysia: Sweet and Maxwell Asia, 2003).

49 Sch 1. For the international dimensions of the PDPO, *see* Berthold and Wacks (n 48 above), Ch 2 "The International Exchange of Personal Data"

50 "Data user" is defined in s 2 as "a person who, either alone or in common with other persons, controls the collection, holding, processing or use of the data"

51 Principle 1(1) in Schedule 1.

52 *Ibid.*, Principle 1(2).

53 *Ibid.*, Principle 2(1).

54 *Ibid.*, Principle 2(2).

55 *Ibid.*, Principle 3. "Data subject" is defined in s 2(1) as "the individual who is the subject of the data". The term "prescribed consent" used in Principle 3 is defined in s 2(3).

56 Principle 4 in Schedule 1.

regards his policies and practices in relation to personal data.[57] DPP 6 confers on a data subject the right to access his personal data held by a data user.[58]

An individual who suffers damage, including injury to feelings, as a result of a contravention of the principles or other requirements in this ordinance may seek compensation.[59] The contravention of a requirement laid down in the body of the PDPO (for example, unjustified refusal to comply with a data access request, which is a contravention of section 19 in addition to being a contravention of DPP 6) – but *not* the contravention of merely a DPP (for example, collection of more data than necessary or collection by means which are unfair in the circumstances) – constitutes an offence.[60] An aggrieved individual may complain to the Privacy Commissioner for Personal Data (PC), an independent authority established to investigate complaints and otherwise administered in the ordinance.[61] Where the PC opines that a contravention is being or has been committed, he may issue an enforcement notice to direct the data user to take steps to prevent a repetition or continuation of the contravention.[62] Failure to comply with an enforcement notice constitutes an offence.[63]

Applicability of PDPO to Telephone Tapping

For the PDPO to be engaged, "personal data" must be involved:

> "'Personal data' means any data – (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable."[64]
>
> "'Data' means any representation of information (including an expression of opinion) in any document."[65]
>
> "'Document' includes a written document, disc, tape, film and any other audio or visual device."[66]

Thus, a tape or disc from which it is practicable to identify the speakers or any living individuals mentioned in the conversations would amount to personal data. Not only the speakers, but also all the other living individuals

57 *Ibid.*, Principle 5.
58 *Ibid.*, Principle 6. For definition of "data subject", *see* (n 59 above).
59 S 66.
60 None of the offences created in s 64 is constituted by the contravention of a principle in Sch 1.
61 Part II.
62 S 50.
63 S 64(7).
64 S 2.
65 *Ibid.*
66 Definition of "document" in s 2 of PDPO.

who can be identified, will be "data subjects", who may seek remedies provided for in the PDPO.

In so far as telephone tapping involves the collection of personal data, the operation of section 33 of Telecommunications must comply, first and foremost, with DPP 1. In regard to DPP 1(1), a law enforcement agency may be considered to be collecting excessive personal data if telephone tapping is done after sufficient evidence has already been collected to establish an unlawful act. However, the principle does not prevent the agency from continuing the privacy-invasive measure in the name of crime prevention or the security of Hong Kong (eg to prevent the further leakage of official secrets to the press).

The requirement of DPP 1(2)(a) for collection to be by lawful means does not indicate that the mode of collection must be positively authorised by law. Otherwise, the vast majority of personal data collection activities in our society, which are done with the data subjects' consent without relying on any legal authority, would contravene the principle. There is no policy justification for such a disruption to existing practices in the society. DPP 1(2)(a) means no more than that the means of collection is not against any legislation or common law.[67] As discussed earlier, there is nothing in the legislation (other than the HKBORO) or common law to render telephone tapping by the Government unlawful.

On the requirement under DPP 1(2)(b) for collection to be by means which are fair in the circumstances, the PC adopts – in the context of employee monitoring – the principle of proportionality (ie the intrusion into privacy should be proportionate to the benefits of monitoring) and the principle of transparency (ie those liable to be monitored should be made aware of the data to be collected, the circumstances in which monitoring may be conducted and the purpose of monitoring).[68] More specifically, he has expressed the opinion, in reply to an enquiry on whether an employer may monitor the telephone conversations of an employee, that the approach "is to ask whether the purpose to be achieved justifies the use of that means in that case" and that "relevant to this issue is whether less privacy-intrusive means are available to achieve the same result".[69] The PC has also advised, in the context of using hidden cameras to monitor possible child abuse by domestic helpers, that "hidden cameras for monitoring are warranted only

67 The PDPO was enacted as a result of the Law Reform Commission, Report on *Reform of the Law Relating to the Protection of Personal Data* (Hong Kong: Government Printer, Aug 1999). Para 9.17 of the report states that "'lawful' would mean neither prohibited by statute nor a civil wrong"

68 Office of the Privacy Commissioner for Personal Data, A Draft Code of Practice on Monitoring and Personal Data Privacy at Work: Consultation Document, para 1.2.3. Available at http://www.legco.gov.hk/yr01-02/english/panels/ha/papers/ha0412cb2-1348-e.pdf, last accessed on 7 June 2003.

69 Case No. 199804574 on the PC's website at http://www.pco.org.hk/english/casenotes/case_enquiry2php?id=13, last accessed on 2 June 2003.

where there are signs of behavioural changes or signs of injury leading to a reasonable suspicion of abuse".[70]

Presumably, the PC – and hopefully, also the courts – will adopt the same principles to assess whether telephone tapping for the purpose of crime prevention and detection or in the interests of the security of Hong Kong is consistent with DPP 1(2). Given the secrecy adopted by the Government, it is doubtful whether the operation of section 33 can be said to comply with the principle of transparency. On the other hand, a case-by-case examination is necessary to establish whether the principle of proportionality is complied with. The stand taken by the Government in relation to the LRC's recommendations to regulate interception of communications gives rise to suspicion that the principle may not feature in the Government's internal guidelines.

The recommendations in question, formulated probably with DPP 1(2)(b) and the principle of proportionality in mind, are as follows:

> "6.8 A warrant authorizing interception of communications should be issued only if the judge is satisfied that –
>
> (a) there is reasonable suspicion that an individual is committing, has committed or is about to commit a serious crime, or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong; and
> (b) there is reasonable belief that information relevant to the investigation will be obtained through the interception; and
> (c) the information to be obtained cannot reasonably be obtained by less intrusive means.
>
> 6.9 In reaching a conclusion on the appropriateness of issuing a warrant, the judge should have regard to the following factors:
>
> (a) the immediacy and gravity of the crime or the threat to public security in respect of Hong Kong, as the case may be;
> (b) the likelihood of the crime or threat occurring; and
> (c) the likelihood of obtaining the relevant information by the proposed interception."[71]

The LRC's paragraph 6.8 was reflected in the Government's White Bill.[72] The Government's reason for not including the recommendation in

70 Case No. 20009383 on the PC's website at http://www.pco.org.hk/english/casenotes/case_enquiry/2php?id=117, last accessed on 30 May 2003.
71 LRC's Report on *Privacy* (n 2 above), p 100.
72 *See* clause 6(2)–(4) in the White Bill attached to the Security Bureau's consultation paper (n 10 above).

paragraph 6.9 was that as the grounds for applying for judicial warrants had been clearly spelt out, "it was not necessary for the designated judge to have regard to other factors."[73] The effect of not having regard to "other factors" appears to be that once any of the grounds mentioned in paragraph 6.8 applies, the judge may issue a warrant even if the intrusion of privacy is disproportionate to the gravity of the offence committed or likely to be committed. Why bother to argue against the LRC's recommendation if it is merely considered to be "not necessary"? One suspects that the Government probably does not apply the proportionality test and does not wish to make any change in future.

Without the proportionality test, the recommendation in LRC's paragraph 6.8 will permit telephone tapping to be used even for some minor offences. In the White Bill, "serious crime" is defined as "any offence punishable by a maximum period of imprisonment of not less than 7 years."[74] Thefts, including shoplifting, are subject to maximum imprisonment for 10 years.[75] Telephone tapping may be justified for the purpose of detecting thefts of billions of dollars committed by sophisticated manipulation of a company's accounts. However, would it be justified, and would it comply with DPP 1(2)(b), if it were used to detect a first-time shoplifter who has stolen goods worth several hundred dollars?[76]

Where telephone tapping under section 33 is conducted in contravention of DPP 1(2)(b) or any other provision in the PDPO, the latter, which was enacted after section 33, prevails pursuant to the common law doctrine of implied repeal. A victim may seek compensation for damages, including injury to feelings.[77] In addition, in order to prevent continuation or repetition of the unjustified intrusion, he may complain to the PC and request an enforcement notice be issued.[78] If the PC refuses to issue such a notice, the complainant may appeal to the Administrative Appeal Board.[79]

Inadequacies of PDPO

Though the PDPO may be invoked by persons who are or suspect themselves to be the victims of telephone tapping, the protection it can provide is inadequate in several aspects. First, the PDPO "protect(s) the privacy of individuals

73 See para 6(f) of minutes of LegCo Panels (n 8 above).
74 See clause 2 of White Bill (n 76 above).
75 S 9 of Theft Ordinance (Cap 210).
76 A safeguard against the anomaly would be to include in the relevant legislation an express provision for the proportionality test. Another would be to define "serious crime", as in s 81(3)(b) of the UK's Regulation of Investigatory Powers Act 2000, in terms of the sentence which can reasonably be imposed on an adult first offender.
77 S 66 of PDPO.
78 S 50 of PDPO empowers the PC to issue enforcement notices.
79 S 47(4) of PDPO.

in relation to personal data"[80] and not privacy in general. It does not apply where no "data" is involved – for example, where a law enforcement agency monitors telephone conversations without recording them on a "document" and all collected information is passed on by word of mouth within the agency.

Secondly, even where the conversations are recorded, the act may not amount to "personal data collection" and DPP 1 may not be engaged. In *Eastweek Publisher Limited and Eastweek Limited v Privacy Commissioner for Personal Data*, the Court of Appeal held, by two to one, that "(i)t is ... of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify".[81] Thus, if a law enforcement agency records a telephone conversation for the purpose of monitoring the activities of an organization (eg to ascertain whether it is affiliated to a foreign political organisation or an organisation banned in the mainland on ground of national security) and keeps the records in the database in such a way that they can be retrieved by reference to the name of the organisation but not the name of any individual, the *Eastweek* ruling would have it that no "personal data collection" is involved. Put it another way, the records relate to an organisation and not any living individual. They are not "personal data" unless and until they are used in a manner which identifies any individuals related thereto.

Thirdly, given the secret nature of telephone tapping, an ordinary citizen would not be able to obtain the necessary evidence to institute civil proceedings for contravention of DPP 1 or other provisions in the PDPO. He will have to turn to the PC. Yet, there is a limitation to the PC's investigatory powers. Section 57 of the PDPO provides for personal data to be exempted from certain provisions of the PDPO if they are held by or on behalf of the Government for the purposes of safeguarding the security, defence or international relations in respect of Hong Kong *and* compliance with the provisions likely to prejudice such legitimate interests. Where a complaint relates to such data, the Chief Executive or the Chief Secretary for Administration may issue a certificate and direct the PC, under subsection (5), not to carry out an investigation – a direction which he shall comply with. Matters relating to security, defence and international relations may therefore be put beyond the reach of the PC. Yet, they are precisely those on which ordinary citizens have the least trust in the Government's willingness to respect individuals' rights.

Fourthly, even where the PC's investigation has established a contravention of the PDPO, he has no authority to award or provide legal assistance for the complainant to seek compensation. The complainant has to institute civil proceedings on his own. The data protection principles are

80 Long title of PDPO. Emphasis added.
81 [2000] 2 HKLRD 83, at p 90, per Ribeiro JA.

phrased in general terms and the above discussion on DPP 1(2)(b) serves to illustrate the need for the courts to read much into the principles before finding a contravention. The result of litigation is uncertain. The compensation which may be obtained – for example, where the complainant may have suffered no damage other than injury to feelings – may be small. An ordinary citizen may find it not worthwhile to go to court and risk being ordered to pay substantial legal costs in case he loses.

Finally, the PDPO is completely useless in protecting against possible abuse by the subordinate organs of the Central People's Government (CPG). According to section 66 of the Interpretation and General Clauses Ordinance, no Ordinance "shall ... be binding on the State unless it is therein expressly provided or unless it appears by necessary implications that the State is bound thereby". The "State" includes the HKSAR Government and the CPG's subordinate organs in Hong Kong that do not exercise commercial functions.[82] Three such subordinate organs have been established: the Office of the Commissioner of the Ministry of Foreign Affairs, the Hong Kong Garrison of the Chinese People's Liberation Army and the Liaison Office of the Central People's Government.[83] Section 3(1) of the PDPO provides that the PDPO binds "the Government", which means the HKSAR Government.[84] There is no express provision to bind other organs of the "State". In determining whether the CPG organs are bound by "necessary implications", the question to consider is whether the legislature intends that they be so bound.[85] It can be inferred from the reference in section 3(1) to only "the Government" that the legislature does not intend the other State organs to be bound.

It would be appropriate to add, at this point, another effect of section 66 of the Interpretation and General Clauses Ordinance. Since neither the Telecommunications Ordinance contains any express provision to bind the CPG subordinate organs nor do they appear to be so bound by necessary implication, the offence provisions created therein which may regulate telephone tapping[86] do not apply to the CPG offices. Though there is no indication whatsoever that the CPG offices conduct surveillance, the lacuna will understandably cause concern, especially to Hong Kong activists who campaign for improving human rights standards in the Mainland.

HKBORO Binding on CPG Subordinate Organs?

For someone intending to seek remedies for unjustified telephone tapping by

82 Definition of "State" in s 3 of Interpretation and General Clauses Ordinance.

83 Legislative Council Secretariat, "Information paper on applicability of Ordinances to the offices set up by the Central People's Government in the Hong Kong Special Administrative Region" (LC Paper No. CB(2)1744/00-01, 8 June 2001), para 6.

84 Definition of "Government" in s 3 of Interpretation and General Clauses Ordinance.

85 Francis Bennion, *Statutory Interpretation* (London, Dublin and Edinburgh: Butterworths, 2002), p 167.

86 *See* nn 45–48 above.

the Government or the CPG organs in Hong Kong, the HKBORO offers the best chance. Section 6 enables the courts to order, in respect of any contravention of the BOR, any remedies which are within their powers. Since the HKBORO binds the Government and public authorities,[87] it may fill the large gap left by the PDPO in regulating possible privacy-intrusive activities by the CPG organs.

The term "public authorities" is not defined in the legislation. Nor has any comprehensive definition emerged through judicial interpretation. In *Hong Kong Polytechnic University and Others v Next Magazine Publishing Ltd and Another*,[88] the High Court, in concluding that the Polytechnic University is a public authority, held that:

> " ... for a body to be a public authority within the meaning of section 7(1) of the Bill of Rights Ordinance, it is not sufficient for it to be entrusted with functions to perform for the benefit of the public and not for private profit: there must be something in its nature or constitution, or in the way in which it is run, apart from its functions, which brings it into the public domain. It is unnecessary ... to identify what that might be: it may take the form of public funding, of a measure of governmental control or monitoring of its performance, or some form of public accountability. But something which brings it into the public domain there must be."[89]

In *Tse Wai Chun Paul v Solicitors Disciplinary Tribunal*,[90] the Court of First Instance (CFI) held that though the Solicitors Disciplinary Tribunal performed certain public functions and might be provided financial support from general revenue, it was not a "public authority".[91] The Court of Appeal (CA), while upholding the CFI's decision that the Tribunal was not obliged to conduct hearings in public, found it unnecessary to consider whether or not the Tribunal was a "public authority". It did say, however, that it was not persuaded that the CFI's ruling on the question was wrong.[92]

87 S 7(1) of BORO.

88 [1996] 6 HKPLR 117.

89 *Ibid.*, pp 122–123. The High Court's decision – that the Polytechnic University, being a public authority, was debarred by the BORO from suing for defamation – was overturned by the Court of Appeal, which held that the common law preventing a local authority from suing from defamation did not apply to a public authority, assuming that the Polytechnic was one. *See Hong Kong Polytechnic University and Others v Next Magazine Publishing Ltd and Another* [1997] 7 HKPLR 286. The appeal decision did not overrule what the High Court said about the meaning of "public authority" but one of the appeal judges did express doubt on whether the University is a "public authority" *Ibid.*, at 291, per Litton VP.

90 Case No. HCAL 636/2001 (Court of First Instance, 27 Aug 2001), last accessed via the Judiciary's website at http://legalref.judiciary.gov.hk/ on 22 July 2003.

91 *Ibid.*, para 61.

92 *Tse Wai Chun Paul v Solicitors Disciplinary Tribunal and Another*, Case No. CACV3174A/2001 (Court of Appeal, 11 Sept 2002), last accessed via Judiciary's website at http://legalref.judiciary.gov.hk on 22 July 2003, para 27.

The CFI in both *Hong Kong Polytechnic University* and *Tse Wai Chun Paul* admitted it had difficulty in defining "public authority" and the CA in both cases chose not to express any definitive view on the question. Adopting for the moment the criteria floated by the CFI in the former case, can it be argued that CPG offices in Hong Kong are not "public authorities" because they are not financed by public funds of Hong Kong, not subject to control or monitoring by the HKSAR Government and not accountable to the public of Hong Kong? Probably not. The ultimate test appears to be whether there are matters about an organisation which "bring (it) sufficiently into the public domain or imbue it with such a public character that it can properly be called a public authority".[93] The CPG organs are set up under BL Article 22(2) for performing functions within the responsibility of the sovereign power under the principle of "one country, two systems". Even if that were insufficient for them to be regarded as "public authorities", the term would have an unduly narrow meaning. Given the ordinary usage of the term, most reasonable persons would probably regard the CPG subordinate organs to be more in the nature of "public authorities" than the Polytechnic University. As the HKBORO was introduced after the 1989 Tiananmen incident, partly with the view of boosting Hong Kong people's confidence in the future, it would be reasonable to infer that the legislature intends the ordinance to protect the people from excesses by not just the HKSAR Government but also the Central Government's representatives.[94]

BOR to Protect Against Telephone Tapping by Government and Public Authorities

The right to privacy – and this means privacy in general and not just privacy in relation to personal data – is protected under BOR Article 14. It reproduces, word for word, ICCPR Article 17, which corresponds to EHRC Article 8. The ECHR has held that the tapping of an office telephone, and not just one installed at home, can also amount to interference with privacy.[95] As has

93 *Ibid.*

94 The point about boosting confidence was merely touched upon during LegCo's debate of the Bill (eg by Hon Mrs Miriam Lau, Hong Kong Legislative Council Official Report of Proceedings for meeting held on 27 June 1990, p 1831). Legislators probably chose not to mention it in order to avoid antagonising China into scrapping the HKBORO after the reversion of sovereignty. That appears to explain why Hon Martin Lee, who normally expresses great concern about certainty of the law, was content to leave the term "public authorities" undefined despite observing the confusion it might create. *See* Hong Kong Legislative Council Report of Proceedings for meeting held on 5 June 1991, p 2330.

95 *Niemietz v Germany* (1993) 16 EHRR 97. It was held that references to "home" and "private life" in ECHR Art 8 included certain aspects of an individual's professional or business life, especially where a confidential relationship existed. There is also a series of cases to the effect that telephone calls made from business premises as well as from the home may fall within the references to "private life" and "correspondence" in Art 8(1) of the EHRC. *See Halford v United Kingdom* (n 33 above), para 44.

been reasoned earlier, telephone tapping also amounts to restriction of the freedom of expression. The argument has more force where the tapped telephone belongs to a reporter or a press organisation. In European jurisprudence, an order for a journalist to disclose his source of information has been held to be a restriction of press freedom.[96] Telephone tapping has the effect of a reporter's source of information being disclosed, without the source's consent, to a third party. The right to freedom of expression is protected under BOR Article 16. The fact that action may lie for breach of Article 16, and not just Article 14, may help to refute the possible argument that the telephone tapping in a particular case targets an organisation and therefore does not interfere with an individual's privacy rights.

Practical Issues in Enforcing BOR

A person who sues for breach of the HKBORO may apply for legal aid. If he passes the merits test, the Director of Legal Aid may waive the means test.[97]

In the circumstances, the HKBORO covers the first, second, fourth and probably, also the fifth inadequacies of the PDPO. That still leaves the third one. The main obstacle to taking actions against telephone tapping is that a person may have purely suspicion, but not sufficient evidence, that his telephone has in fact been tapped. While the PC's investigatory powers may be restricted when it comes to cases involving defence, security and international relations, there is simply no investigatory authority established for enforcing the HKBORO.[98] The gap can perhaps be filled by the Ombudsman.

96 In *Goduin v United Kingdom* (1996) 1 BHRC 81, the ECHR held that a court order requiring a reporter to disclose the identity of his source and the fine imposed on him for refusing to comply amounted to an interference with his right to freedom of expression.

97 S 5AA of Legal Aid Ordinance.

98 The question of establishing a human rights commission to investigate complaints was debated by the Legislative Council before HKBORO was enacted. Members held divided opinions on the need and functions and decided not to let the matter delay the passage of the ordinance (*see* Hon Selina Chow's speech in Hong Kong Legislative Council Official Report of Proceedings for meeting held on 5 June 1991, p 2308). The Government's reasons for not setting up the commission were the costs involved, the need to give detailed consideration to its functions and composition and that the case had been weakened by the decision not to apply the HKBORO to inter-citizen disputes (*see* Chief Secretary's speech, *Ibid.*, p 2337). The matter was revived several years later by legislator Hon Anna Wu but her proposal for the commission was rejected by the Executive Council on the ground that its establishment would anger China (*see* Carole J. Petersen, "Equality as a Human Right: The Development of Anti-discrimination Law in Hong Kong" 34 *Colum J Transnat'l L* 335, at 375). The treaty monitoring bodies for ICCPR and International Covenant on Economic, Social and Cultural Rights, after considering the HKSAR's reports under the two treaties, expressed concern about the lack of an independent body to investigate complaints and monitor compliance with the treaties (*see* United Nations documents CCPR/C/79/Add.117 dated 12 Nov 1999, para 9 and E/C.12/1/Add.58 dated 21 May 2001, paras 15(d) and 32). The HKSAR Government maintained that the existing framework for implementing human rights provisions through the judiciary, legal aid system and Ombudsman should continue but undertook to listen to public opinions and review the need to reconsider its position (*see* speech by Secretary for Home Affairs in Hong Kong Special Administrative Region Legislative Council Official Record of Proceedings for meeting held on 13 June 2001, pp 6111–6112). The HKSAR Government's preparation of the next report under ICCPR has revived interest in the subject (*see* "Barristers cite slow progress on rights", *South China Morning Post*, 12 April 2003, p 6).

Conducts which breach the BOR are "unlawful" and therefore, fall within the meaning of "maladministration", which is within the Ombudsman's jurisdiction.[99] The Ombudsman – at least the previous one – saw the protection of human rights to be within his roles.[100] Yet, the summaries of complaint cases included in The Ombudsman's annual reports covering the period from July 1997 to March 2002 contain nothing to suggest that the office takes into account any human rights provisions when considering complaints.

In any case, the Police Force, which is the law enforcement agency most likely to resort to telephone tapping for the purposes of detecting crime or otherwise protecting the security of Hong Kong, is outside the Ombudsman's jurisdiction.[101] Complaints against the Police Force are investigated by the Complaints Against Police Office (CAPO), a unit of the Force itself. The investigations are monitored by the Independent Police Complaints Council. In case a person complains about telephone tapping purely on the basis of his subjective suspicion, one doubts that CAPO will go to the extent of investigating whether any branch of the Force has in fact conducted surveillance on the complainant. CAPO, understandably, would avoid the complaints channel being used by criminals to obtain information on police operations against them.

The question whether telephone tapping had actually taken place arose in three European cases. In *Klass v Germany*,[102] where the German government stated that no surveillance had been mounted on the applicants and the applicants did not adduce any evidence to challenge the statement, the ECHR made the following observations:

> "(T)he contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this ... To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore, as the Delegates rightly pointed out, *this menace of surveillance can be claimed in*

99 Johannes Chan, "Hong Kong's Administrative Complaints System" [1996] 3 *HKLJ* 339, at 357.

100 Office of the Ombudsman, Hong Kong, China, *The Ombudsman and the Protection of Human Rights in Hong Kong* (Hong Kong, Jan 1998), para 38. However, Mr Andrew So, the then Ombudsman, later gave the impression that he was inclined to confine himself to "a number of important fundamental human rights which (he) may come across in (his) work and which should warrant (his) special attention." See Office of the Ombudsman, Hong Kong, China, *The Tenth Annual Report of The Ombudsman, Hong Kong, China* (Hong Kong, June 1998), para 5.18.

101 The effect of s 7 read in conjunction with Sch 1 of The Ombudsman Ordinance (Cap 397) is that the Ombudsman may investigate actions taken by the Police Force only if the actions relate to the compliance with the Code on Access to Information published by the Government.

102 (1980) 2 EHRR 214.

itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8."[103]

"Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to '*[claim] to be the victim* of a violation' of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants *were actually the victims* of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions."[104]

In *Malone*,[105] the applicant believed that his correspondence and telephones had been intercepted for several years. The UK government admitted that one single conversation revealed in an earlier criminal trial against the applicant had been obtained by interception and conceded that the applicant belonged to a class of persons whose communications were liable to be intercepted under the relevant legislation.[106] In finding for the applicant, the ECHR stated that:

"(T)he 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 ... This being so, the Court ... does not consider it necessary to inquire into the applicant's further claims that both his mail and his telephone calls were intercepted for a number of years."[107]

The LRC commented on *Malone* as follows:

"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."[108]

103 *Ibid.*, para 37. Emphasis added.
104 *Ibid.*, para 38. Emphasis in original text.
105 *See* n 22 above.
106 *Ibid.*, para 16.
107 *Ibid.*, para 64.
108 LRC's Report on *Privacy* (n 2 above), para 3.32.

In *Halford*,[109] a case after the LRC's report, the ECHR appeared to have changed its approach to one which is less protective of the individual's rights. Ms Halford alleged that her telephones at home and at the office had been tapped. The Interception of Communications Act 1985 regulated the interception of calls on the public telecommunications system, which did not include the internal telecommunication system in her office. She adduced evidence of her office telephone being tapped. The ECHR awarded damages for distress. Similar evidence was not available to support her allegation about the tapping of her home telephone. One would have expected that following *Klass* and *Malone*, the ECHR would hold the existence of phone tapping practice to be in itself an interference with the phone users' privacy right and then proceed to examine whether the 1985 Act constituted the "law" required to render the interference lawful. Instead, the ECHR held that the applicant had not established a reasonable likelihood of any surveillance having been applied to her home telephone and that, therefore, there was no violation of her right to privacy.[110] Distinguishing from *Klass*, it decided:

> "(T)he essence of Ms Halford's complaint, unlike that of the applicants in *Klass v Germany* ... was not that her Article 8 rights were menaced by the very existence of admitted law and practice permitting secret surveillance, but instead that measures of surveillance were actually applied to her. Furthermore, she alleged that the Merseyside police intercepted her calls unlawfully, for a purpose unauthorised by the 1985 Act."[111]

In a case alleging violation of Article 14 or Article 16, or both, of the BORO, will Hong Kong courts be persuaded by the European jurisprudence to rule that section 33 of the Telecommunications Ordinance does not meet the foreseeability test to be regarded as "law"? As regards the evidence required to establish an allegation of violation, will the courts adopt the libertarian stand in *Klass* and *Malone* such that the existence of section 33 and the practice as admitted by the Government in the LegCo in themselves pose a menace to all telephone users? Or, will they follow *Halford* such that the onus is on the complainant to establish that there is a reasonable likelihood of any interception having been carried out? The answers to the questions will determine whether the HKBORO is capable of providing adequate protection against telephone tapping by the Government and public authorities.

If the Hong Kong courts were to decide, as in *Halford*, that the evidence required depends on the specific allegations actually made, potential complainants could easily tailor their allegations to suit the ruling. The

109 *See* n 33 above.
110 *Ibid.*, paras 57–60.
111 *Ibid.*, para 57.

Government might then be inundated by countless claims for inestimable damages. All telephone tapping would have to stop even where it is necessary for the prevention or detection of serious crime. On the other hand, if the courts were to require evidence of actual telephone tapping, it would, to use the LRC's words, "reduce the right to privacy to a nullity" and the end result would be to undermine public confidence in the courts' determination to protect human rights. A compromise would be to require the complainants to produce *some* evidence to raise a suspicion that he has been subjected to surveillance. Depending on the threshold, the option would give rise to either of the above adverse consequences.

None of the eventualities would be in the public interest. The public interest dictates that the Government must take immediate actions to put such surveillance measures on a proper constitutional footing. After all, six years have elapsed since the Government completed the public consultation on the White Bill.

Conclusion

To the extent that telephone tapping involves interfering with telecommunications systems, the intrusive measures, if carried out by the private sector, can be addressed by the relevant offences under the Telecommunications Ordinance. Persons suspecting their telephones to have been tapped – for example, by their employers – may also be able to obtain remedies under the PDPO.

The offence provisions in the Telecommunications Ordinance, which are not binding on the Government, do not protect citizens from possible abuse of the power, conferred on the Chief Executive and authorised public officers under section 33, to order interception. Telephone tapping amounts to interference with the right to privacy and the right to freedom of expression. Section 33, which says next to nothing about the circumstances in which and conditions on which covert telephone tapping may be ordered, does not meet the standard set out in European jurisprudence as regards the "law" that is required to justify such interference. The Government has been reticent about any detailed guidelines which may exist on the exercise of the discretion. In any case, such guidelines, if existing at all, would not constitute the "law" required.[112]

[112] In *Khan v United Kingdom* (2000) 8 BHRC 310, para 27, the ECHR held that the Home Office Guidelines (described in paras 16–18), though available in the library of the House of Commons and disclosed by the Home Office on application, were not legally binding and not "directly publicly accessible" The Guidelines, therefore, could not be regarded as "law"

Where telephone tapping involves the collection of personal data, the PDPO may be able to provide victims with remedies against possible abuse by all data users in both public and private sectors – except the CPG's subordinate organs in Hong Kong, which are not bound by the PDPO. However, a vital deficiency of the PDPO is that when it comes to matters relating to security, defence and international relations in respect of Hong Kong – and these are matters on which the public has the least confidence in the Government's acting judiciously – the Chief Executive and the Chief Secretary for Administration may direct the PC not to investigate a complaint. Without the PC's intervention, it is impossible for citizens to collect the evidence required to substantiate a contravention.

A victim of telephone tapping, imaginary or real, may have no better alternative than relying on the HKBORO. The ECHR's rulings in *Klass*, *Malone* and *Halford* are persuasive. There does not appear to be much to distinguish between Europe and Hong Kong, a world city whose government claims a human rights record comparable to that of the most advanced jurisdictions in the world. If Hong Kong courts were to follow *Klass* and *Malone*, the Government's admission of the telephone tapping practice would in itself be sufficient evidence to support an allegation of contravention of the BOR. In case *Halford* were followed and a plaintiff bore the burden of proving a reasonable likelihood of telephone tapping having actually taken place, citizens would have little protection.

The risk of a law enforcement agency being sued for telephone tapping exists every day. The judiciary will be put in the invidious situation of having either to deny the law enforcement agencies a useful ammunition in the detection of serious crime, or to reduce the right to privacy a nullity. Either way, the judiciary will attract criticisms and its image may suffer. A responsible government will therefore not risk anything which may undermine public confidence in the judiciary, especially when the rule of law is our biggest competitive advantage in the struggle for economic survival.

Immediate actions to replace section 33 with legislation dedicated to regulate interception of communications are in order. The Hon James To's Interception of Communications Ordinance (ICO) (Cap 532), enacted while Hong Kong was still a British colony, would not be sufficient for the purpose. To get round Royal Instructions paragraph XXIV, which provided that any legislative proposal with a charging effect on public revenue required the Governor's consent, the ICO does not provide for the establishment of a Supervisory Authority to investigate complaints. This weakness renders the ICO inadequate in protecting citizens against possible abuse. The Government's White Bill published in February 1997, though not incorporating all the LRC's recommendations, is closer to the mark. Now

that six years have passed since the Government completed public consultation, one expects the Government to be able to introduce a Blue Bill into the LegCo any time now.