THE LAW REFORM COMMISSION OF HONG KONG

REPORT

PRIVACY:
THE REGULATION OF
COVERT SURVEILLANCE

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

March 2006

The Law Reform Commission of Hong Kong was established by the Executive Council in January 1980. The Commission considers for reform such aspects of the law as may be referred to it by the Secretary for Justice or the Chief Justice.

The members of the Commission at present are:

Chairman: ***Mr Wong Yan-lung, SC, Secretary for Justice***

Members: ***The Hon Mr Justice Andrew Li, Chief Justice***
Mr Tony Yen, SBS, JP, Law Draftsman
Dr John Bacon-Shone
The Hon Mr Justice Bokhary, PJ
Professor Albert Chen, JP
Mr Anthony Chow, SBS, JP
Professor Y K Fan, BBS, JP
Professor Michael McConville
Mr Paul Shieh, SC
Ms Anna Wu, SBS, JP
Mr Benjamin Yu, SC, JP

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

20/F Harcourt House
39 Gloucester Road
Wanchai
Hong Kong

Telephone: ***2528 0472***
Fax: ***2865 2902***
E-mail: ***hklrc@hkreform.gov.hk***
Website: ***http://www.hkreform.gov.hk***

THE LAW REFORM COMMISSION OF HONG KONG

REPORT

PRIVACY: THE REGULATION OF COVERT SURVEILLANCE

CONTENTS

Preface

_____

Background

1. In October 1989, the Law Reform Commission was asked:

> *—ð 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 Commission appointed a sub-committee to examine the current state of legislation and to make recommendations. The members of the Privacy Sub-committee are

Dr John Bacon-Shone *(Chairman)*	Associate Dean, Faculty of Social Sciences; Director, Social Sciences Research Centre, The University of Hong Kong

Mr Don Brech	Principal Consultant, Records Management International Limited (Former Director, Government Records Service)
Professor Johannes M M Chan (from November 2001)	Honorary Senior Counsel, Dean, Faculty of Law, The University of Hong Kong
Mrs Patricia Chu, BBS, JP (till April 2001)	Former Deputy Director of Social Welfare (Services), Social Welfare Department
Mr A F M Conway	Chairman, Great River Corporation Limited
Mr Edwin Lau	Chairman, Hooray Holdings Limited (Former Assistant General Manager & Head of Strategic Implementation Asia Pacific, HSBC)
Mr Robin McLeish (from February 2000)	Barrister-at-law
Mr Barry Mortimer, GBS (Chairman of sub-committee from 1990 till August 1999)	Non-Permanent Judge, Court of Final Appeal
Mr James O"Neil	Deputy Solicitor General (Constitutional), Department of Justice
Mrs Kathy Ng Ma Kam-han (from April 2001 to April 2003)	Assistant Director (Elderly) Social Welfare Department
Mr Peter So Lai-yin (till November 2001)	Former General Manager Hong Kong Note Printing Limited
Mr Richard Tang Hau Sing (from April 2005)	Director of Crime and Security Hong Kong Police Force
Professor Raymond Wacks (Chairman of sub-committee from August 1999 to December 2001)	Emeritus Professor of Law and Legal Theory, The University of Hong Kong
Mr Wong Kwok-wah	Editor, Asia Times-On-Line (Chinese version)

Miss Amy Chan, Senior Government Counsel, was the secretary to the sub-committee during the preparation of this report.

3. Since being given its original terms of reference, the Law Reform Commission"s Privacy sub-committee has completed studies of a number of aspects of privacy, resulting in final Commission reports on *Reform of the Law Relating to the Protection of Personal Data* (published in August 1994), *Privacy: Regulating the Interception of Communications* (published in December 1996), *Stalking* (October 2000), *Privacy and Media Intrusion* and *Civil Liability for Invasion of Privacy* (both published in December 2004). The one remaining aspect of the privacy reference is surveillance. The sub-committee issued a combined consultation paper on surveillance and interception of communications in 1996, and while final recommendations were subsequently made in respect of interception of communications, the question of surveillance was deferred for later consideration. This report now sets out the Commission"s final recommendations in respect of covert surveillance.

The requirement for a legislative framework

The guarantees of the right to privacy

4. Article 29 of the Basic Law of the Hong Kong Special Administrative Region prohibits arbitrary or unlawful search or intrusion into a resident"s home or other premises. Article 30 provides that the privacy of communications may not be infringed except to meet the needs of public security or of investigation into criminal offences. Article 39 of the Basic Law guarantees that the provisions of the International Covenant on Civil and Political Rights ("the ICCPR") as applied to Hong Kong shall remain in force.[1]

5. Article 17 of the ICCPR as incorporated in Article 14 of the Hong Kong Bill of Rights (Cap. 383, Part II) ("HKBOR") provides that no one shall be subjected to "*arbitrary or unlawful interference with his privacy, family, home or correspondence*", and that everyone has the right to the protection of the law against such interference.

6. In order to provide adequate and effective protection against arbitrary or unlawful intrusion into the privacy of individuals, we recommend that a legislative framework should be set up for the regulation of covert surveillance and the covert obtaining of personal information.[2]

---

1 Article 39(2) of the Basic Law further provides that the rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law. Such restrictions shall not contravene the provisions of Article 39(1), which guarantees that the ICCPR shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region.

2 The purpose of surveillance is to capture information relating to the individual, but the intrusive nature of the process means that surveillance is objectionable whether or not any information is obtained as a result.

The general principles for regulation of covert surveillance

Legality

7. The law regulating such surveillance activities must be readily accessible and precise so that individuals will be aware of the circumstances and the conditions under which public authorities may resort to the use of such intrusive powers.[3]

Proportionality

8. Covert surveillance constitutes an interference with the right to privacy. Any interference with such a fundamental right would only be lawful if it is for the pursuit of a legitimate aim and that any measures taken to restrict that right must be proportionate to the legitimate aim to be achieved.[4] There must be criteria in place to determine when and under what circumstances it is justified to interfere with the right to privacy.

Accountability

9. The exercise of intrusive powers must be subject to adequate and effective safeguards which include such elements as prior scrutiny,

---

[3] As held by the Court of Final Appeal in *Gurung Kesh Bahadar v Director of Immigration* [2002] 2 HKLRD 775 and *Shum Kwok Sher v HKSAR* [2002] 2 HKLRD 793, "*a law must be formulated with a sufficient degree of precision – just how must depends upon the nature and content of the subject matter in question – so that the individual is given some indication how he may regulate his conduct*". See also *Leung Kwok Hung v HKSAR* FACC 1/2005 (Court of Final Appeal), at paras 25-29. In *Malone v United Kingdom* (1985) 7 EHRR 214, the European Court of Human Rights held that a system under which telephone and mail interception was conducted under a warrant issued by the Secretary of State, with no statutory framework, afforded insufficient legal protection to satisfy the requirement of the right to privacy guaranteed under Article 8 of the European Convention on Human Rights: "…*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 view of the obscurity and uncertainty as to the state of the law in this essential aspect, the Court cannot but reach a similar conclusion to that of the Commission [namely that Article 8 which guaranteed the right to respect for private life had been violated]. 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.*" See also *Kruslin v France* (1990) 12 EHRR 528: "*It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated*."

[4] Any restriction on a fundamental right must be proportionate to the aims sought to be achieved by the restriction: *Ming Pao Newspapers v Attorney General of Hong Kong* [1996] AC 907 (Privy Council), *HKSAR v Ng King Siu* [2000] 1 HKC 117 (Court of Final Appeal). In *X v The Commissioner of the Independent Commission Against Corruption* HCCM 49/2003, it was held by the Court of First Instance, at paras 16-19, that under Article 14(1) of the HKBOR, "*[a] person is given a right to privacy that can only be interfered with in accordance with law and not even then if it is exercised in an arbitrary fashion…the law which limits the rights must be part of a properly passed statute, or be an established part of the common law. …The limiting law must also conform with international law's prescribed forms for laws on human rights. In that it must be clear and accessible to everyone….It must not be arbitrary (although that is already specifically mentioned in A.14(1))…*"

independent oversight, and access to remedy before an independent court or tribunal.[5]

An integrated approach to regulating intrusion

10. We take the view that an integrated approach should be adopted to the regulation both of the interception of communications and of covert surveillance to provide effective protection against undue interference with privacy.

The structure of this report

11. In accord with Article 29 of the Basic Law which prohibits arbitrary or unlawful intrusion into a resident"s home or other premises, we take the view that criminal sanctions should afford protection against covert surveillance and the covert collection of personal information which involve intrusion into "private premises" without lawful justification or consent. We have defined the conduct that would constitute a criminal offence in relation to surveillance in Chapter 1 of this report.

12. We take the view that covert surveillance is necessary for law enforcement purposes and for the protection of the public security in Hong Kong. In Chapter 2, we recommend the establishment of a regulatory system which sets out the circumstances in which a warrant issued by the Court of First Instance should be required for such intrusions to be lawful and the situations where an internal authorisation granted by an authorising officer of a designated law enforcement agency would be sufficient for those purposes.

13. We examine in Chapter 3 the grounds upon which a warrant or an internal authorisation for covert surveillance may be issued and the matters that should be taken into account by the judge or the issuing authority in assessing whether the application is for a legitimate purpose and whether it complies with the proportionality requirement. The procedures for the application and the renewal of a warrant or internal authorisation, their duration, and the procedures for emergency applications are explained in Chapter 4.

14. In Chapter 5, we consider the admissibility of materials obtained from covert surveillance as evidence in legal proceedings. Recommendations

---

[5] As stated by the European Court of Human Rights in *Klass v Federal Republic of Germany* (1978) 2 EHRR 214: "*The Court must be satisfied that…there exist adequate and effective guarantees against abuse. This assessment…depends on all the circumstances of the case, such as the nature, 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*." It has also been held in *X v The Commissioner of the Independent Commission Against Corruption* HCCM 49/2003, at para 18, that "*…there should be adequate safeguards and effective remedies provided by law against illegal or abusive applications of the limitation.*"

relating to the retention, disclosure and destruction of materials obtained from surveillance are made in Chapter 6.

15. The question of whether it is necessary to notify the person who is subject to covert surveillance of that fact is discussed in Chapter 7 of the report.

16. In Chapter 8, we recommend the creation of an independent supervisory authority, which would review the issue of warrants or internal authorisations as a means of providing effective safeguards to the regulatory system. The supervisory authority would also deal with complaints from aggrieved persons in relation to covert surveillance.

17. We recommend in Chapter 9 that an annual public report should be furnished to the Legislative Council and a confidential report to the Chief Executive. These reports would serve to increase transparency and accountability in relation to covert surveillance activities carried out by the law enforcement agencies.

Terminology

18. Unless the context requires otherwise, references to "the sub-committee" are to the Law Reform Commission‟s Privacy Sub-committee, and "the consultation paper" refers to the sub-committee‟s consultation paper on "*Privacy: Regulating Surveillance and the Interception of Communications*", published in 1996. The consultation paper can be accessed through the Commission‟s website at *http://www.hkreform.gov.hk/reports/index.htm*.

Chapter 1

Proposed criminal offences relating to covert surveillance

General approach to criminal sanctions

1.1 In recommending what surveillance conduct should be regarded as unlawful and subject to criminal sanctions we have borne the following considerations in mind:

(a) Social need

Conduct should not be criminalised unless there is a social need and it is essential to do so. Broadly drawn criminal offences could lead to abuse.

(b) Establishing norms

Where social need is made out, criminal sanctions usefully establish social norms and proscribe unacceptable conduct.

(c) Deterrence and retribution

The existence of criminal offences would have a deterrent effect, even if no prosecution were ever brought.

(d) Systematic investigation

Attaching criminal sanctions to unacceptable conduct enables the Individual to obtain police assistance in investigating and remedying wrongdoing.[6]

The scope of the regulation of surveillance

1.2 The Privacy Sub-committee recommended in its consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications* a statutory regulatory framework incorporating three proposed criminal offences:

---

[6] Para 56, Introduction to the consultation paper.

(1) trespass into private premises with intent

It would be an offence for a person to enter private premises as a trespasser with intent to observe, overhear or obtain personal information therein.[7]

(2) physical intrusion into private premises by means of a technical device

It would 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.[8]

(3) placing or using of a technical device outside private premises with intention of monitoring activities held on the premises

It would 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.[9]

In reviewing the proposals in the consultation paper, and the responses to that paper, we are conscious that the consultation exercise was carried out ten years ago. Since then, there have been legislative developments in a number of other jurisdictions, including Australia and the United Kingdom. In the United Kingdom, for instance, there has been considerable debate over the years, both in Parliament and in the community at large, as to the regulation of covert surveillance and interception of communications. The results of the consultation exercise carried out in Hong Kong in 1996 must accordingly be viewed with that caveat.

The first offence: trespass into private premises with intent to observe, overhear or obtain personal information

1.3 The responses to the consultation paper all supported the creation of the offence of entering private premises as a trespasser with intent to observe, overhear or obtain personal information.[10]

---

7 Para 1.34, consultation paper.

8 Para 1.37, consultation paper.

9 Para 1.70, consultation paper.

10 For instance, the Bar Association agreed to the creation of the proposed offence involving trespass into private premises.

Definition of private premises

1.4 For the purposes of the proposed offence, the consultation paper defined "private premises" to mean any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. It also included bedrooms (but not other areas) in a hotel and those parts of a hospital or nursing home where patents are treated or accommodated, school premises, commercial premises, aircraft, vessels and vehicles from which the public are excluded.[11]

1.5 The general response to the consultation paper was that the definition of "private premises" for the purposes of the proposed criminal offences was too wide.[12] We have taken account of the submissions, and have decided to revise the definition of "private premises" to include only:

> *"any premises, or any part of premises, occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation; any room hired by the proprietor of a hotel or guesthouse to guests for lodging;*[13] *or those parts of a hospital or nursing home where patients are treated or which are used as sleeping accommodation."*

1.6 We have accordingly removed "School premises, commercial premises, aircraft, vessels and vehicles from which the public are excluded" from the original definition of "private premises".

1.7 Concern was also expressed as to whether passageways, lift lobbies, roofs, balconies, and the common areas in buildings would fall within the definition of "private premises". We do not intend that our reference to private premises should include any common area to which an individual is allowed access in connection with his use or occupation of such premises.[14]

---

11 Para 1.42, consultation paper.

12 The Hong Kong Journalists Association submitted that the definition was not adequately tuned to local circumstances as few people have gardens, outbuildings or adjacent parklands in Hong Kong. The term "*commercial premises … from which the public are excluded*" was regarded as having too broad a coverage. Some respondents submitted that the inclusion of commercial premises, aircraft, vehicles and schools in the definition would restrict the media in their investigation and reporting of matters of public interest. It was further suggested that the inclusion of "*aircraft, vessels and vehicles from which the public are excluded*" would unduly hamper the effectiveness of law enforcement.

13 Section 2 of *the Hotel and Guesthouse Accommodation Ordinance* (Cap 349) defines "hotel" and "guesthouse" as: "*any premises whose occupier, proprietor or tenant holds out that, to the extent of his available accommodation, he will provide sleeping accommodation for any person presenting himself who appears able and willing to pay a reasonable sum for the services and facilities provided and is in a fit state to be received*."

14 This provision is adapted from section 48(7)(b) of the United Kingdom *Regulation of Investigatory Powers Act 2000*.

Meaning of "personal information"

1.8 "Personal information" was not defined in the consultation paper.[15] However, there have been judicial observations in recent decisions in the Court of Appeal[16] and the House of Lords[17] in the United Kingdom to the effect that "private information" about a person is information which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved.

1.9 We also note that one of the constituent elements of covert surveillance under the Executive Order No 1 of 2005 is that the surveillance is likely to result in the obtaining of any "*private information about the person*".[18]

---

15 The term "personal information" has, however, been defined in legislation in other jurisdictions and by academics. Professor Wacks, in *Privacy and Press Freedom*, at page 23, defines "personal information" as: *"those facts, communications, or opinions that relate to the individual and which are of such a nature that it would be reasonable to expect him to regard as intimate or sensitive, and therefore to want to withhold or at least to restrict their collection, use or circulation."* Under the *Personal Information Protection and Electronic Documents Act* of Canada enacted in 2000, "personal information" is defined under Part 1 of the Act to mean: *"information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."* The United Kingdom *Freedom of Information Act 1997* defines "personal information" in section 2 as: *"…information about an identifiable individual that – (a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual, or (b) is held by a public body on the understanding that it would be treated as confidential."* Such information as defined under the Act includes information relating to the educational, medical, psychiatric or psychological history of the individual, information relating to his financial affairs and information relating to his employment or employment history.

16 In *Douglas v Hello Limited*, Judgment dated 18 May 2005, at para 83, the Court of Appeal stated: "*What is the nature of private information?' It seems to us that it must include information that is personal to the person who possesses it and that he does not intend shall be imparted to the general public. The nature of the information, or the form in which it is kept, may suffice to make it plain that that the information satisfies these criteria."*

17 In *Campbell v MGN Ltd* [2004] 2 AC 457, the issue was whether there had been wrongful disclosure of private information. The House of Lords, by a majority of three to two, held that the details of the plaintiff's attendance at Narcotics Anonymous, together with the photographs, constituted private information the publication of which amounted to a breach of confidence. In the course of the judgement, the House of Lords referred to the frequently cited test applied in *Australian Broadcasting Corp v Leach Game Meats Pty Ltd* (2001) 185 ALR 1, at 13, para 42, to decide whether information disclosed was "private": *"An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford. Certain kinds of information about a person, such as information relating to health, personal relationships, or finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved…."* It was further suggested by Lord Hope, at para 96, that "*if the information is obviously private, the situation will be one where the person to whom it relates can reasonably expect his privacy to be respected. So there is normally no need to go on and ask whether it would be highly offensive for it to be published*." Lord Nicholls in the same case made the comment, at para 21, that: *"…Essentially the touchstone of private life is whether in respect of the disclosed facts the person had a reasonable expectation of privacy."*

18 Section 2 of the Executive Order No 1 of 2005, cited as the *Law Enforcement (Covert Surveillance Procedures) Order*.

Use of technical device not essential

1.10 We agree with the recommendation in the consultation paper that the use of a technical device should not be a necessary ingredient of the first offence.[19]

The revised recommendations

1.11 The offence proposed in the sub-committee"s consultation paper required that the offender had entered private premises as a trespasser with the intent of observing, overhearing or obtaining personal information. The offence did not require that the offender"s actions were covert, and we agree with this approach. The proposed offence should equally be committed where there is an overt intrusion on private premises, as where, for instance, a photographer forces his way into a person"s home to take photographs.[20]

1.12 A key element in the offence proposed in the consultation paper was that the offender had "entered" the private premises as a trespasser. There may be circumstances, however, in which an individual enters private premises legitimately but subsequently outstays his right to remain. For instance, a guest who refuses to leave after being asked to do so by the occupant would at that stage become a trespasser. To cover such situations, we believe that an appropriate adjustment should be made to the wording of the first offence. We therefore recommend that the first offence should consist of:

> *—entering or remaining on private premises as a trespasser with intent to observe, overhear or obtain personal information."*

Where a law enforcement agency wished to enter premises for these purposes, it would need to obtain a search and seizure warrant if its actions were to be overt, or a covert surveillance warrant if it intended to act covertly.

---

19 Para 1.39, consultation paper.

20 A case illustrating the situation is *Kaye v Robertson* [1991] FSR 62. The plaintiff was a well-known actor. He suffered severe injuries to his brain and was hospitalised in a private room which had a notice asking visitors to see a member of the staff before visiting. The defendant journalists ignored the notice and entered the room. Although the plaintiff apparently agreed to talk to them and did not object to them taking photographs inside the room, it was confirmed at the civil trial that the plaintiff was in no fit condition to be interviewed or to give any informed consent to be interviewed. The court held that there was no right to privacy in English law and accordingly there was no right of action for breach of a person"s privacy. An injunction for malicious falsehood was granted which only afforded limited protection. As pointed out by Lord Bingham, the real complaint was that the plaintiff"s privacy had been the subject of a monstrous invasion but for which the interview would never have been obtained at all. The act of the journalists in this case would have fallen within the bounds of the first offence proposed in the present report. They had entered without the permission of the staff. The personal information and photos were obtained or taken from a person who was not capable of giving consent. The journalists had obviously entered the room as trespassers. The private room in the hospital would certainly fall within the definition of "private premises" in the proposed offence. The conduct would therefore constitute an offence , namely that of entering or remaining on private premises as a trespasser with intent to observe, overhear or obtain personal information as proposed in the present report.

The second offence: physical intrusion into private premises by means of a technical device

Recommendations in the consultation paper

1.13 The consultation paper recommended 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. This is commonly referred to as the "bugging" of premises and involves the placement or use of a surveillance device, such as a camera, microphone, or similar device, in the premises.

The responses to the consultation paper

1.14 The Bar Association was in favour of the proposed offence. One respondent objected on the ground that the offence could be committed by a person who accidentally left a camera in another person's premises.

Intent to obtain personal information

1.15 The rapid technological advances in the field of communications mean that the availability of devices capable of being used to record, monitor, or listen to conversations or activities for the purpose of obtaining personal information has greatly increased. It would no longer be appropriate to render such conduct criminal without requiring proof that the placement, use, servicing or removal of such a device was carried out with intent to obtain personal information.

1.16 We therefore recommend that a person should only be guilty of the offence of placement or use of a surveillance device inside private premises where the offence is committed with intent to obtain personal information.

Consent of the lawful occupant

1.17 Under the original proposal in the sub-committee's consultation paper, the offence of physical intrusion into private premises by means of a technical device would be committed where the intrusion was "*without the consent of the lawful occupier*". A person would be exempt from criminal liability if he had the consent of the lawful occupier to carry out the prohibited act of surveillance.

1.18 Article 29 of the Basic Law prohibits "*arbitrary or unlawful*" intrusion into a resident's home or other premises. It is clearly necessary to specify in the legislation the categories of persons by whom, and the

circumstances in which, valid consent may be given to intrusion into private premises by means of a surveillance device.

1.19 Where the premises are occupied for residential purposes by a sole occupant, a person would be guilty of the offence of intrusion into private premises with a technical device unless consent has first been obtained from that sole occupant, who must be an adult.

1.20 Where more than one occupant resides in the same private premises, we consider a distinction should be drawn between the situation where a number of persons occupy the same accommodation independently of each other (as in the case of a dormitory in a hostel) and the situation where a number of persons occupy the same accommodation together (as in the case of a family household). In the former situation, we do not think that one of the lawful occupants should be able to give consent to, or carry out, covert surveillance of the others with the use of a technical device. In contrast, in the latter situation we consider that one lawful occupant should be able to give consent to, or carry out, covert surveillance of the other occupants with the use of a technical device. That would not constitute a criminal offence, subject to the proviso that there should be an express prohibition on covert surveillance in changing rooms, rooms used wholly or in part for sleeping accommodation and toilet, shower or bathing facilities, without the consent of the adult occupant concerned.[21] These are all areas where a person would reasonably expect to have a high degree of privacy and as such merit particular consideration.

1.21 Where the owner or lawful occupant of private premises considers that there is a need to undertake covert surveillance in a prohibited area in relation to a suspected criminal offence committed by another occupant of the premises, the proper approach would be to report the matter to a law enforcement agency. Where a law enforcement agency needs to undertake covert surveillance in those areas, justifications should be provided by an officer of the law enforcement agency concerned to the judge or the authorising officer in the application for a warrant or internal authorisation.

Revised recommendations[22]

1.22 We recommend that where the private premises concerned are occupied or used by any person, however temporarily, for residential or sleeping purposes or otherwise as living accommodation, consent to the use of a technical device for surveillance inside the premises may be given:

(a) in the case of premises lawfully occupied by one person, or occupied jointly by more than one person, by any one of those lawful occupants who is an adult; and

---

21 Section 9(3)(b), *Workplace Video Surveillance Act 1998*, New South Wales. The same provision has been retained in the *Workplace Surveillance Bill 2004* (NSW) Clause 9.

22 We recommend later in this chapter that the second and third offences should be combined into a single offence, but we discuss here first the elements of the second offence.

(b) in the case of premises lawfully occupied by more than one person independently of each other, only by every lawful adult occupant.

We further recommend that in respect of private premises used as living accommodation there should be an express prohibition on covert surveillance in changing rooms, rooms used wholly or in part for sleeping accommodation, and any toilet, shower or bathing facilities, other than where authorised by a warrant or internal authorisation.

1.23 The effect of these recommendations would be, for instance, that the placement or use of a device for covert surveillance purposes inside a hotel room hired to guests for lodging would be an offence unless consent for so doing had been obtained from the guest or, where the room was occupied by more than one guest, any one of them. In contrast, in premises such as a hostel or a home for the aged, where a number of individuals occupy premises independently of each other, the recommendations would preclude a single occupant giving consent to, or carrying out, covert surveillance of the others.

1.24 Having reviewed the original recommendation in the consultation paper, we maintain the view that the offence of physical intrusion into a hospital or nursing home using a technical device should be restricted to those parts of a hospital or nursing home where patients are treated or which are used as sleeping accommodation. Where the act was done with intent to obtain personal information other than for medical purposes, it would constitute criminal conduct unless the consent of the person who is the subject of the surveillance has been given.[23]

Meaning of "sense-enhancing, transmitting or recording device"

1.25 There was criticism that the consultation paper"s proposal did not make clear what kind of equipment would fall within the definition of "*sense-enhancing, transmitting or recording device*".

1.26 We have examined the definitions of surveillance devices in the legislation in the United Kingdom[24] and Australia.[25] We do not think it

---

[23] We note that bylaw 7(1)(f) of the *Hospital Authority Bylaws* (Cap 113A) prohibits a person from taking any photograph, film or video picture which depicts a patient in a hospital without the consent of such patient. A person who contravenes any of the above provisions commits an offence and is liable to a fine of $2,000 and to imprisonment for three months. However, we are minded to restrict the application of the offence to the area where patients are treated, or which are used as sleeping accommodation, instead of applying it to any part of a hospital or nursing home.

[24] "Surveillance device" is defined under section 48(1) of the Part II of the *Regulation of Investigatory Powers Act* in the United Kingdom to mean "*any apparatus designed or adapted for use in surveillance*". Surveillance activities are defined under section 48(2) as including: "(*a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the assistance of a surveillance device*."

necessary to define the term "*sense-enhancing, transmitting or recording device*". Whether any device would fall within the category of a "*sense-enhancing, transmitting or recording device*" would depend on its use in the particular circumstances of the case. We accordingly adopt the recommendation in the consultation paper that it should be an offence to use a "*sense-enhancing, transmitting or recording device*" with intent to obtain personal information without the consent of the lawful occupant of private premises. We should stress that we do not intend that the use of everyday devices such as spectacles or hearing aids, designed to correct sensory deficiencies, should be caught by the offence. We mean instead to target devices which enhance sensory perception beyond normal human capability.

The third offence: placing or using a technical device outside private premises with the intention of monitoring activities on the premises

Recommendations in the consultation paper

1.27 The consultation paper recommended 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.[26] Under this proposed offence, criminal sanctions would only attach to surveillance conducted outside private premises which utilises technical devices and targets individuals within private premises.

1.28 The consultation paper further proposed that the requirement for the presence of intent to monitor the activities or data inside private premises "*would exclude accidental surveillance or hacking".* Whether such intent exists "*will be a question of fact and there will be situations where the surveillance device can be shown to be targeting particular premises*".[27]

---

25 ~~S~~Surveillance device*"* is defined under section 3 of the *Surveillance Devices Act 2000* of the Northern Territory of Australia to mean *~~a~~ data surveillance device, a listening device, an optical surveillance device or a tracking device"*. A *"data surveillance device"* means *"~~a~~ apparatus, device, instrument, machine or piece of equipment capable of being used to record or monitor the information being put on to or retrieved from a computer"*. A *"listening device"* means *~~a~~n apparatus, device, instrument, machine or piece of equipment capable of being used to record, monitor or listen to a private conversation or words spoken to or by a person in a private conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome his or her impairment and enable him or her to hear only sounds ordinarily audible to the human ear"*. An *"optical surveillance device"* means *"~~a~~ apparatus, device, instrument, machine or piece of equipment capable of being used to visually record, monitor or observe a private activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome his or her impairment and enable him or her to see only sights ordinarily visible to the human eye"*. A *"tracking device"* means *~~a~~n apparatus, device, instrument, machine or piece of equipment capable of being used to determine or monitor the geographical location of a person, vehicle or object"*.

26 Para 1.70, consultation paper.

27 Para 1.72, consultation paper.

The submissions

1.29 The Bar Association agreed to the creation of the proposed offence. The Hong Kong Press Photographers Association took the view that the offence might criminalise certain innocent conduct, and cited the example of a person taking a photo of something seen without the assistance of any technical device while standing in a public place. The Association was of the view that where a person chose not to protect their privacy, the freedom of others should not be restricted, nor should their exercise of that freedom be penalised. There was also concern from the media that reporters taking photos from outside of persons in an aircraft, vessel or private vehicle would be committing a criminal offence.

Revised recommendations

1.30 We consider that where an individual or his property is in plain view and is visible to the naked eye, the use of binoculars or a telephoto-lens camera to observe or record his actions does not normally infringe the individual"s expectation of privacy. However, if a technical device is used to collect data which would otherwise be shielded from observation but for the use of the device, such conduct could constitute an invasion of privacy.[28]

Merging of the second and third offences

Recommendations

1.31 We take the view that the elements of the second and third proposed offences are similar. We therefore recommend that the offence of "*placing, using or servicing in, or removing from, private premises of a sense-enhancing, transmitting or recording device without the consent of the lawful occupier*" should be combined with the offence of "*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*".

1.32 The only difference between the two offences is that, in relation to the second offence, it would constitute criminal conduct for a person "to place, use, or service in, or remove from*" inside* private premises a surveillance device with intent to conduct covert surveillance of persons inside the premises, whereas in relation to the third offence it would be an offence for a person to place or use a technical device *outside* private premises with the same intent. We consider the distinction as to whether the device was

[28] This was the view adopted by the Law Reform Commission at para 6.56 of the report on *Civil Liability for Invasion of Privacy*. Under the first example cited by the Hong Kong Press Photographers Association, the taking of a photo of a woman on the balcony of her premises would not constitute an offence if she was visible to the naked eye or in plain view of the public.

placed or used "inside" or "outside" the private premises is artificial and unnecessary, taking into account the similar nature of the two offences.

1.33 Upon consolidation, it would be an offence for a person:

> *~~to~~ place, use, service or remove a sense-enhancing, transmitting or recording device (whether inside or outside private premises) with the intention of obtaining personal information relating to individuals inside the private premises in circumstances where those individuals would be considered to have a reasonable expectation of privacy."*

An individual would generally be considered to have a reasonable expectation of privacy that he would not be subject to surveillance from inside private premises, but whether or not such an expectation can reasonably be said to exist in respect of surveillance from outside private premises will depend on the particular circumstances.

1.34 So long as the observation is made by an officer who has the right to be where he is, and encompasses only that which is in plain view, the fact that the observation was made with the use of binoculars does not transform it into an unlawful intrusion into privacy.[29] Observations with binoculars do not deprive the person observed of any reasonable expectation of privacy.[30] However, if what is observed could not be seen without the use of a telescopic aid, then that amounts to an invasion of the right of privacy of the person observed.[31]

1.35 We consider that the observation with the use of technical aids of that which is in plain view even without the use of those aids should not constitute an offence. The validity of the observation of persons or property in plain view turns upon the subject"s reasonable expectation of privacy, rather than upon the means used to view it. As long as the object viewed is visible to the naked eye, technological aids of whatever type may be used without infringing the person"s constitutional rights.[32]

1.36 We agree with the principle that when objects are in the plain view of an individual outside private premises, the use of photographic equipment to record the presence and nature of the objects observed should not constitute an offence.[33]

---

29 68 American Jurisprudence 2d, at page 712, para 104. See also *US v Gibson*, 636 F 2d 761 (DC Cir 1980).

30 68 American Jurisprudence 2d, at page 712, para 104. See also *US v Whaley*, 779 F 2d 585 (11th Cir 1986)

31 68 American Jurisprudence 2d, at page 712, para 104. See also *State v Ward* 62 Haw. 509, 617 P.2d 568 (1980).

32 68 American Jurisprudence 2d, at page 712, para 104.

33 68 American Jurisprudence 2d, at page 712, para 107.

Meaning of "reasonable expectation of privacy"

1.37 Whether the conduct of covert surveillance from inside or outside private premises into the activities or conversations of persons inside the private premises amounts to an offence would depend on whether there is any infringement of the reasonable expectation of privacy of the persons concerned. As explained in the consultation paper, a person's reasonable expectation of privacy can be broadly categorised as having the following three aspects:

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

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

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

when in all the circumstances he has a reasonable expectation that the intrusion in question will not occur.[34]

1.38 The sub-committee considered in its consultation that the "reasonable expectation of privacy" test was "*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 …. Finally we doubt if the broader test has any prospect of generating the political support necessary for it to become law."*[35]

1.39 Much has changed since the sub-committee expressed that preliminary view in 1996. Firstly, there have been developments in the law relating to the concept of "reasonable expectation of privacy" in a number of jurisdictions. In the United States, for instance, the Supreme Court has applied the test to surveillance cases.[36] In Canada, privacy legislation in

---

34 Para 53, Introduction to consultation paper.

35 Para 1.60, consultation paper.

36 *United States v Katz* 389 U.S. 347 (1967) is a landmark decision by the Supreme Court of the United States under which the reasonable expectation of privacy test was introduced in surveillance cases. *Katz* was concerned with an investigation into an illegal betting scheme. The FBI taped a microphone to the roof of a public phone booth. The microphone was connected by a wire to an FBI listening post. The microphone did not wiretap the telephone line. It merely recorded Katz's end of the conversations, picking up what an eavesdropper might have heard had he stood near the booth when Katz used the phone. The government

British Columbia and Newfoundland provides that the nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others. In its 1998 report, the Irish Law Reform Commission recommended that a new tort of privacy-invasive surveillance should protect a reasonable expectation of privacy. The Irish Commission proposed that in determining whether the privacy of a person has been invaded by means of surveillance, the court should consider the extent to which that person was reasonably entitled to expect that he would not be subjected to such

---

played the recordings of Katz placing bets at trial. The majority of the Supreme Court took the view that although there was no physical trespass into the phone booth, a person "*who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world*." In *United States v Cuevas-Sanchez* 821 F.2d 248, at 251 (5th Cir. 1987), the police installed a video camera atop a power pole overlooking the appellant's 10-foot high fence bordering the back of the yard. Officers observed the removal of drugs from vehicles in the appellant's yard. The court took the view that the appellant did manifest a subjective expectation of privacy in his backyard through the erection of fences around it to screen the activities within from the view of casual observers and that the area monitored by the camera fell within the curtilage of his home. The court ruled that the act constituted an infringement upon the personal and societal values protected by the Fourth Amendment: "*To measure the government's intrusion we must consider the expectations of society. … This type of surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the spectre of the Orwellian state. Here, … the government's intrusion is not minimal. … Here the government placed a video camera that allowed them to record all activity in [the applicant]'s backyard. … [The applicant]'s expectation to be free from this type of video surveillance in his backyard is one that society is willing to recognize as reasonable*." In *California v Ciraolo*476 U.S. 207 (1986), investigators flew an aeroplane above the defendant's backyard and looked down from public airspace to see whether the defendant was growing marijuana in the yard. The United States Supreme Court held that the surveillance did not violate the property owner's reasonable expectation of privacy because the plane was flown "within public navigable airspace" and "in a physically nonintrusive manner". In *Kyllo v United States* 533 U.S. 27 (2001), law enforcement officers suspected that marijuana was being grown in the home of the petitioner. In order to determine whether an amount of heat emanating from the petitioner's home was consistent with the use of high-intensity lamps required for indoor marijuana growth, those officers used a thermal imager to scan the petitioner's home. The scan took only a few minutes and was performed from the passenger seat of the officers' vehicle across the street at the back of the house. The scan showed that the roof of the garage and a side wall of the petitioner's house were relatively hot compared to the rest of the house and substantially warmer than neighbouring houses. Pursuant to a warrant issued by a Federal Magistrate, the law enforcement officers searched the petitioner's home and found an indoor growing operation involving more than 100 plants. The petitioner was indicted on one count of manufacturing marijuana. He sought to suppress the evidence seized from his home on the ground that the warrant was invalid as it had been issued in part upon the thermal imaging which was evidence obtained from an unlawful search. The United States Supreme Court, in a majority opinion delivered by Justice Scalia, held the thermal imaging to have been an unlawful search. The court took the view that limits had to be imposed to restrict the adverse effect of the advancement of technology on the protection of the privacy of individuals from unlawful search or surveillance: *—It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. ... The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy. … [I]n the case of the search of the interior of homes - the prototypical and hence most commonly litigated area of protected privacy - there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area"… constitutes a search – at least where (as here) the technology in question is not in general public use."*

surveillance having regard to all the relevant circumstances.[37] In our own report on *Civil Liability for Invasion of Privacy* in 2004, we considered that "*the notion of reasonable expectation of privacy is the core of an intrusion tort*."[38]

1.40 The second change that impacts on the sub-committee"s preliminary conclusion in 1996 is the narrowing of the scope of the criminal offences we now propose. The definition of "private premises" is now to be constituted by clearly defined and specific locations, and there is to be an exemption from criminal liability where the consent of a lawful occupant of the "private premises" has been obtained or where prior authorisation has been granted to the relevant law enforcement agencies. Both these revisions to the sub-committee"s original 1996 proposals mean that the scope of the application of the proposed consolidated offence would be restricted to limited and definable circumstances where infringement of privacy is considered to be serious.

1.41 In addition, we have clarified the test to be applied and the factors to be considered in determining whether a person is entitled to a "reasonable expectation of privacy" in any particular circumstances. The test for determining whether a person has a reasonable or justifiable expectation of privacy has two limbs. The first is whether the person"s conduct exhibits a subjective expectation of privacy. The second is whether the person"s subjective expectation of privacy is one that society is willing to recognise as reasonable.[39] We have set out the factors that are relevant in assessing whether an individual"s expectation of privacy is reasonable at paragraph 2.43 of Chapter 2 of this report.

1.42 Having taken into account these changes, we take the view that the application of the "reasonable expectation" test of privacy is sufficiently precise for inclusion in the proposed consolidated offence.

Application of the proposed offences

1.43 We recommend that a person should not be guilty of either of the proposed offences if the act falling within the scope of the proposed offence was carried out pursuant to a warrant issued in accordance with the statutory provisions specified under Chapter 2 of this report.

1.44 As discussed at paragraphs 1.22 to 1.24 above, a person should not be guilty of the second proposed offence if the act falling within the scope of that offence was carried out with the consent of a lawful occupant of the "private premises".

---

37 *Report on Privacy*, Irish Law Reform Commission (1998), Ch 10, Head 1(3)(i), at 121.

38 Report on *Civil Liability for Invasion of Privacy*, Hong Kong Law Reform Commission (2004), para 6.26.

39 68 *American Jurisprudence* 2d *Searches and Seizures*, at para 327.

Unauthorised disclosure of surveillance materials

1.45 In Chapter 6, we recommend the creation of a further offence in respect of a person who discloses without authorisation materials obtained through duly authorised covert surveillance.

Defences

Recommendations in the consultation paper

1.46 The consultation paper considered what defences should apply to the proposed new offences and pointed out that:

> *"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."*[40]

1.47 The sub-committee recommended in the context of the interception of communications that it should be a defence if the interceptor believed on reasonable grounds that a communicant had consented.[41]

Recommendations in the report on Privacy: Regulating the Interception of Communications

1.48 The establishment of a public interest defence was suggested by some respondents to the consultation paper on the regulation of surveillance and interception of communications. The Hon James To proposed that the defence should be available to an accused who intercepted a communication in good faith and clearly in the public interest. The Hong Kong Journalists Association believed that such a defence was necessary to prevent the proposed legislation from being applied in an offensive manner.[42]

1.49 The Commission's report on Privacy: Regulating the Interception of Communications noted that "None of the overseas laws we examined provide for an exemption on the ground that the interception was executed in

---

40 Para 5.49, consultation paper.

41 Para 5.50, consultation paper.

42 Para 6.87, report on *Privacy: Regulating the Interception of Communications*.

the public interest,"[43] and concluded that: "We are not in favour of adopting a general defence of public interest".[44]

1.50 Some respondents to the consultation paper commented that physical intrusion by the media should not be prohibited where the publication of the information obtained in consequence of the intrusion was in the public interest.[45] The Commission"s report took the view that there should be a distinction between the act of intrusion and that of disclosure. The Commission agreed that the defence of public interest might be relevant in resolving the issue of disclosure or publication. However, the media had always been subject to limitations on the methods used for news-gathering. The report concluded that no journalist should be allowed to intercept a private communication merely because the publication of the information to be obtained by the interception was justified in the public interest.[46]

1.51 The report reiterated the view that the "publication of information, and the means of obtaining the information, should always be kept separate and distinct."[47] It recommended that:

> *"... interception of communications should be made unlawful unless it is exempted or authorised by the court. Although the media would not be allowed to apply for an interception warrant under our proposals, they may still employ other less intrusive means, or rely on the exception applicable to consensual interception."*[48]

The Interception of Communications Bill

1.52 In the White Bill on *Interception of Communications*, the exemptions to the offence of intentional interception of communications were listed in section 3(2) as follows:

> "*(2) Subsection (1) shall not apply to the interception of a communication —*
>
> *(a) pursuant to a warrant;*
> *(b) …that is intercepted by a law enforcement agency of the Government for the purpose of preventing, investigating or detecting crime or for the security of Hong Kong;*
> *(c) permitted under section 7 [post-application for a warrant];*

---

43 Para 6.89, report on *Privacy: Regulating the Interception of Communications.*
44 Para 6.90, report on *Privacy: Regulating the Interception of Communications*.
45 Para 9.18, report on *Privacy: Regulating the Interception of Communications*.
46 Paras 9.19 - 9.21, report on *Privacy: Regulating the Interception of Communications*.
47 Para 9.21, report on *Privacy: Regulating the Interception of Communications*
48 Para 9.24, report on *Privacy: Regulating the Interception of Communications*.

(d) for a purpose connected with the establishment, maintenance or provision of postal or telecommunication services…;

(g) being any interception to which a party to the communication has consented or to which the person who intercepts reasonably believes that such a party has consented;

(h) being assistance or support provided by a carrier or an employee of a carrier to the Government in connection with an interception authorized under this Ordinance; or

(i) being any interception made pursuant to an Aviation Security Programme…."

The Bill accordingly only provided a defence of consent by a party to the communications.

The Interception of Communications Ordinance (Cap 532)

1.53 Section 3(2) of the Interception of Communications Ordinance provides that a person shall not be guilty of an offence of interception of communications if the communication is intercepted pursuant to a court order, or the person has reasonable grounds for believing that the person to whom, or by whom, the communication is made has consented to the interception.

1.54 Section 3(3) of the Ordinance further provides that a person shall not be guilty of an offence under section 3(1) if the communication is intercepted in accordance with the Post Office Ordinance (Cap 98) or the Telecommunication Ordinance (Cap. 106). Section 3(4) further provides for a public interest defence in the following terms:

> *"In any proceedings against a person for an offence under this section, it shall be a defence to the accused to prove that the interception was conducted in good faith for the purpose of revealing a serious threat to public order or to the health and safety of the public."*

Other jurisdictions

The United States

1.55 In the United States, the *Wiretap Act* prohibits the interception of wire, oral or electronic communications.[49] There are exemptions provided to operators of the communication service, pursuant to a court order, where consent has been given by a party to the communication.[50] There is no general defence on the ground of public interest.

---

[49] Section 2511(1)(c) of the US *Wiretap Act*.

[50] Section 2511(2) of the US *Wiretap Act*.

The United Kingdom

1.56 In the United Kingdom, section 92 of the *Police Act 1997* provides that:

> *"No entry on or interference with property or wireless telegraphy shall be unlawful if it is authorised by an authorisation having effect under this Part."*

This provision empowers the police to enter premises or interfere with property with authorisation. No criminal offence of conducting covert surveillance has been created under the United Kingdom's *Regulation of Investigatory Powers Act 2000*.

Australia

1.57 The *Surveillance Devices Act 2004* sets up a statutory regime regulating the use of surveillance devices for the investigation of offences by the law enforcement agencies. It does not create any general criminal offence which is applicable to the public.

Canada

1.58 Section 184(2) of the *Criminal Code* of Canada provides that the offence of interception of a private communication does not apply to a person who has the consent of the originator or of the intended recipient to the interception; or where interception is carried out in accordance with an authorisation. The offence also does not apply to a person engaged in providing communication services to the public. There is apparently no general defence to the offence of interception of a private communication on public interest grounds.

Revised recommendations

1.59 We have considered carefully whether to provide a defence of public interest. We do not believe that the offences we propose would catch conduct which might legitimately be said to be in the public interest. Nevertheless, we have decided to recommend that it should be a defence to either of the proposed surveillance offences that the accused had an honest belief, and there were reasonable grounds for believing, that:

(a) a serious offence had been, or was being, committed;

(b) the law enforcement agencies would not investigate or prosecute that offence;

(c) evidence of the commission of that serious offence would be obtained through surveillance, and could not be obtained by less intrusive means; and

(d) the purpose of the surveillance was the prevention or detection of a serious offence.

The defence will require both a subjective and an objective element ("honest belief" and "reasonable grounds for believing"). It will be available only to those who genuinely believe that their use of surveillance is in the public interest. An accused who does not believe that a serious crime had, or was being, committed, even though there are reasonable grounds for that belief, will not be able to plead the defence. Likewise, mere honest belief is not sufficient unless there were also reasonable grounds to support that belief. The defence will not be open to an accused who cannot show reasonable grounds for his honest belief.

Chapter 2

The regulatory system

Circumstances in which a warrant is required to conduct covert surveillance

Covert surveillance involving "private premises"

2.1 In Chapter 1 of this report, we have revised the recommendations in the consultation paper *on Privacy: Regulating Surveillance and the Interception of Communications* as to the conduct which would constitute a criminal offence in respect of surveillance. We confirm the consultation paper's recommendation, however, that a warrant should be required to authorise covert surveillance involving "private premises" where such surveillance would otherwise fall within the scope of one of the proposed criminal offences set out in Chapter 1 of this report. In addition, in view of the intrusiveness of such conduct, we recommend that a warrant should generally be required to authorise covert surveillance involving the use of a device on private premises, whether or not that conduct would constitute one of the proposed criminal offences.[1] By "covert", we mean surveillance which is carried out in a manner calculated to ensure that the persons who are subject to the surveillance are unaware that it is, or may be, taking place. There are already well understood mechanisms to regulate the overt intrusion into private premises for the collection of personal information. Such conduct is covered by a search warrant. What we are concerned with here, however, is the covert collection of personal information.

Covert surveillance involving intrusion into "specified premises"

2.2 We have also considered whether any covert surveillance which does not fall within the ambit of the proposed criminal offences may still require regulation by the warrant system. We take the view that where the covert surveillance involves intrusion into school premises, commercial premises, aircraft, vessels and vehicles, from any of which the public are excluded ("specified premises"), even though the conduct no longer falls within the scope of any of the criminal offences proposed in this report, the interference is sufficiently serious to justify a warrant requirement.[2]

---

1 We consider later in this Chapter the authorisation required where the person carrying out the surveillance is himself a participant in the conversation (what may be termed "participant surveillance")..

2 In the consultation paper, "private premises" were defined to extend beyond domestic premises to school premises, commercial premises, aircraft, vessels and vehicles from which the public are excluded. In Chapter 1 of this report we have revised the scope of "private premises" to

2.3 We therefore recommend that any law enforcement agency that wishes to carry out covert surveillance involving intrusion into "specified premises" must apply to the Court of First Instance for a warrant.

Covert surveillance involving acquisition of knowledge of matters subject to legal privilege

2.4 Where acts of covert surveillance are likely to result in the acquisition of knowledge of matters subject to legal privilege, we consider that covert surveillance should only be carried out with a warrant.

2.5 Legal professional privilege is a fundamental right long established in common law. It is now protected under Article 35 of the Basic Law which guarantees that "*Hong Kong residents shall have the right to confidential legal advice*". Legal professional privilege enables a person to make full disclosure to his legal adviser without apprehension that communications made for the purposes of seeking and receiving legal advice may thereafter be subject to disclosure against his will or used to his prejudice. It is vital to the administration of justice. Any encroachment on the privilege affects not only the legal system but has an impact on the broader public interest.[3]

2.6 The seizure and retention of "*items subject to legal privilege*" is expressly prohibited by a number of specific legislative provision, even where the entry by law enforcement officers into premises for search and seizure is authorised by a warrant, unless those items were held with the intention of furthering a criminal purpose.[4] In a decision by the District Court, it was held that the only circumstances in which a law enforcement officer can intercept a privileged conversation is if the officer has grounds to believe that the meeting with the lawyer was concerned with the furtherance of some criminal activity.[5]

---

mean only those premises occupied for residential purposes, any hotel bedroom and those parts of a hospital or nursing home where patients are treated or which are used as sleeping accommodation.

[3] *Pang Yiu Hung Robert v Commissioner of Police* [2002] 4 HKC 579, at 587-589; *R v Derby Magistrates Court, ex p B* [1996] 1 AC 487, at 507

[4] Sections 21(5) and 22 of the *Drug Trafficking (Recovery of proceeds) Ordinance* (Cap 405); sections 2 and 5 of the *Organized and Serious Crimes Ordinance* (Cap 455). "*Items subject to legal privilege*" are defined in those Ordinances as any communications between a professional legal adviser and his client (or representative) made in connection with the giving of legal advice, or made in connection with, or in contemplation of, legal proceedings and for the purposes of those proceedings, and extends to items enclosed with or referred to in communications of that kind.

[5] *HKSAR v Shum Chiu and others* DCCC 687/2004, ruling by Deputy Judge Livesey dated 5 July 2005. It was pointed out by the court that the covert recording by the ICAC of conversations which it knew would be likely to be subject to legal professional privilege amounted to "*a breach of a fundamental condition upon which the administration of justice as a whole rests*". An application for judicial review against the decision of Judge Livesey was made by the Secretary for Justice. The application was heard before Hartmann J with judgment delivered on 22 December 2005 in *Secretary for Justice v Shum Chiu and others* HCAL 101/2005. Hartmann J, at paras 15, 16 and 31 of the judgment explained the nature and application of "legal professional privilege" as follows: "*The common law has long recognised that the right to legal advice is of such importance to the due administration of justice that, if that right is compromised, then justice itself is undermined. As Lord Taylor CJ expressed it in*

2.7 Having considered these issues, we recommend that a warrant should be required to authorise covert surveillance where the law enforcement officers concerned know, or where there are reasonable grounds to believe, that information subject to legal privilege is likely to be acquired in the course of such surveillance.

Covert surveillance involving acquisition of confidential journalistic material

2.8 Where covert surveillance is likely to result in the acquisition of confidential journalistic material, we recommend that a warrant should be required in view of the seriousness of the intrusion.

2.9 The statutory scheme in Part XII of the *Interpretation and General Clauses Ordinance (Cap 1)* restricts access to journalistic material to those persons who are authorised by statute to carry out searches.[6] An application must be made to a judge of the Court of First Instance or District Court either for a production order in respect of the journalistic material or for a warrant to authorise entry onto premises for the search or seizure of journalistic material.[7] The rationale for the special protection accorded journalistic material is that it is in the public interest to preserve the freedom of the press and to protect the confidentiality of the media"s sources of information.[8]

R v Derby Magistrates Court, ex parte B [1996] 1 AC 487, at 507, legal professional privilege is much more than an ordinary rule of evidence, limited in its application to the facts of a particular case; in the common law it is 'a fundamental condition on which the administration of justice as a whole rests'. In Hong Kong, legal professional privilege is protected by the Basic Law as a fundamental human right….If the communications are made in order to obtain advice for a criminal purpose then, of course, legal professional privilege does not attach itself to those communications. This exception applies whether the lawyer is a knowing party or is ignorant of the criminal purpose and is being used as an innocent tool by the client alone and/or with third parties to advance a criminal purpose….That being the case, it must follow, I think, that, if there are objectively cogent grounds for believing that a meeting, which prima facie is protected by legal professional privilege, is in fact to be used in order to further a criminal enterprise – and will not therefore in fact be privileged – then the investigating authorities must be able to discover what has passed at that meeting." See footnote 35 in Chapter 5 of this report for further details of this case.

6 "Journalistic material" is defined in section 82 of Cap 1 as "*any material acquired or created for the purposes of journalism"* which is "*in the possession of a person who acquired or created it for the purposes of journalism*."

7 As stipulated under sections 83 to 85 of Cap 1, approval from a superior officer must be obtained prior to the application. There must be reasonable grounds for believing that an arrestable offence has been committed; that the material is likely to be of substantial value to the investigation of the offence or to constitute relevant evidence in the proceedings; that other methods of obtaining the material have been tried or failed, or have not been tried because they would be unlikely to succeed or would be likely to seriously prejudice the investigation; and that it is in the public interest having regard to the benefit likely to accrue to the investigation that such a warrant should be granted.

8 *Apple Daily Limited v Commissioner of the Independent Commission Against Corruption*, [2001] 1 HKC 295, judgment by the Appeal Committee of the Court of Final Appeal, at pages 304-305: *—[T]he rationale underlying Pt XII, I believe, relates to the important role played by a free and independent press to as public watchdog. The press should be able to speak out on matters of public interest without fear or reprisal, and journalists need to protect the confidentiality of the sources of the information they receive. On the other hand, the legitimate requirements of law enforcement agencies may in exceptional cases make it necessary for*

2.10 Having taken these factors into consideration, we recommend that a warrant should be required to authorise covert surveillance which is likely to result in the acquisition of journalistic material.

Covert surveillance resulting in acquisition of highly sensitive personal information

2.11 We have also considered whether a warrant should be required for covert surveillance undertaken by a law enforcement agency where it is likely to result in the acquisition of personal information of a highly sensitive nature.

2.12 We do not think that it is possible to devise an exhaustive list of what constitutes "highly sensitive personal information". Examples, however, may be given by way of illustration. For instance, information about a person"s medical condition held in confidence;[9] information relating to his intimate private life;[10] or information that he had been receiving spiritual counselling may, under particular circumstances, assume the characteristics of "highly sensitive personal information".

2.13 We appreciate that there are obvious difficulties in establishing statutory provisions of general application in this area where circumstances may vary so widely. However, we take the view that the acquisition of sensitive personal information is of such a level of intrusiveness as to require regulation. We therefore recommend that the primary legislation should require internal guidelines to be established by law enforcement agencies to provide detailed guidance on the undertaking of covert surveillance which is likely to result in the acquisition of "highly sensitive personal information". The guidelines should be approved by the supervisory authority. They should be published and made available to the public. We believe that such guidelines should include the following matters:

---

journalistic materials to be the subject of seizure and inspection. In this sensitive area, Part XII of the IGCO requires a judge of the Court of First Instance or the District Court to hold the balance between these two competing interests." See also *So Wing Keung v Sing Tao Limited*, CACV 245/2004, judgment by Court of Appeal dated 11 October 2004, at para 36.

9 In *Z v Finland* (1997) 25 EHRR 371, at paras 96-97, the European Court of Human Rights took the view that the disclosure of confidential information about a person"s HIV infection might "*dramatically affect his or her private and family life as well as social and employment situation … It may also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic*. *The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued …. In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any state measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection. At the same time, the Court accepts that the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings*."

10 Information which revealed that a person was a drug addict receiving treatment may constitute sensitive personal information: see *Campbell v MGN Ltd* [2004] 2 AC 457.

(a) Where there are reasonable grounds to believe that information likely to be acquired is of a high degree of sensitivity, the law enforcement agency concerned should seek judicial authorisation;

(b) In determining whether any information should be regarded as sensitive personal information, the relevant factors that should be taken into account include, but are not limited to, the following matters:

(i) the place where the intrusion will occur;

(ii) the nature of the information to be obtained by the intrusion;

(iii) the means by which the intrusion will be carried out; and

(iv) the extent to which the privacy of any person is likely to be affected.

(c) An examination as to whether the criteria for the application for a warrant for covert surveillance as set out in Chapter 3 of this report have been satisfied should be carried out prior to the making of any application.

Covert surveillance by a party to the targeted activity

2.14 An issue which falls to be considered is whether a person who is a party to a conversation or activity which takes place inside "private premises" and who carries out an act falling within the scope of either of the proposed criminal offences should be exempt from criminal liability, or whether he should be required to obtain a warrant to authorise his actions. The question would arise where, for instance, an undercover officer used a concealed "bug" to record his conversation with a suspect in private premises. The wider question to consider is whether, because of the inherent intrusiveness of the conduct, *any* surreptitious use of a device on private premises for participant surveillance should require authorisation, regardless of whether it constitutes a criminal offence.

Relevant case law

Dietemann v Time, Inc

2.15 In the US case of *Dietemann v Time, Inc*[11], the reporters for a news magazine gained access by deception to a doctor"s home office, where they secretly photographed and recorded his examination of one of them. The United States Court of Appeal held that under California law the plaintiff could reasonably expect privacy from press photography and recording even though he had invited the reporters, unaware of their true identity, into his home office:

> *—Plaintiff's den was a sphere from which he could reasonably expect to exclude eavesdropping newsmen. He invited two of defendant's employees to the den. One who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves. But he does not and should not be required to take the risk that what is heard and seen will be transmitted by photographing or recording, or in our modern world, in full living color and hi-fi to the public at large or to any segment of it that the visitor may select."*[12]

Sanders v American Broadcasting Companies, Inc.

2.16 In the US case of *Sanders v American Broadcasting Companies, Inc.*[13], an undercover reporter employed by ABC. deliberately obtained employment with a company where the applicant worked. The undercover reporter used a video camera hidden in her hat to covertly videotape her conversations with several co-workers, including the applicant. The Supreme Court of California held that a person who lacks a reasonable expectation of complete privacy in a conversation, because that conversation could be seen and overheard by co-workers (but not the general public), may nevertheless have a claim for invasion of privacy by intrusion based on a television reporter"s covert videotaping of that conversation. The court said at page 9 of the judgment:

> *—..privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law."*

---

11 449 F.2d 245.

12 Above, at 246.

13 (1999) 6/24/99 SC.

2.17 The court went on at page 19 of the judgment:

> *—To summarize, we conclude that in the workplace, as elsewhere, the reasonableness of a person's expectation of visual and aural privacy depends not only on who might have been able to observe the subject interaction, but on the identity of the claimed intruder and the means of intrusion. … For this reason, we answer the briefed question affirmatively: a person who lacks a reasonable expectation of complete privacy in a conversation, because it could be seen and overheard by coworkers (but not the general public), may nevertheless have a claim for invasion of privacy by intrusion based on a television reporter's covert videotaping of that conversation.*
>
> *Defendants warn that the adoption of a doctrine of per se workplace privacy would place a dangerous chill on the press' investigation of abusive activities on open work areas, implicating substantial First Amendment concerns.' We adopt no such per se doctrine of privacy. We hold only that the possibility of being overheard by co-workers does not, as a matter of law, render unreasonable an employee's expectation that his or her interactions within a non-public workplace will not be videotaped in secret by a journalist. In other circumstances, where, for example, the workplace is regularly open to entry or observation by the public or press, or the interaction was that the subject of the alleged intrusion was between proprietor (or employee) and customer, any expectation of privacy against press recording is less likely to be deemed reasonable. …".*

R v Duarte

2.18 The issue of whether the electronic recording of individuals' conversations with undercover police officers and police informers in the absence of judicial authorisation constituted an infringement of section 8 of the Canadian Charter of Rights and Freedoms (which guarantees the right to be secure against unreasonable search and seizure) was considered by the Supreme Court of Canada in *R v Duarte*.[14] The Supreme Court held that the warrantless "participant surveillance" engaged in by the police in that case was unconstitutional.

2.19 The facts of the case in *Duarte* were that as part of an investigation into drug trafficking, the police rented an apartment for a police informer who was working with an undercover police officer. The apartment was equipped with audio-visual recording equipment installed in a wall. Prior to the installation of the equipment, the informer and the undercover officer

[14] [1990] 1 SCR. 30.

consented to the interception of their conversations. The defendant discussed a cocaine transaction with the undercover officer and the informer at the apartment. The undercover officer made notes of this and a subsequent conversation based upon a review of the tapes of the conversations.

2.20 The defendant was subsequently charged with conspiracy to import a narcotic. At trial, he challenged the validity of section 178.11(2)(a) of the Criminal Code of Canada, which excepts from the prohibition on unauthorised electronic surveillance the interception of conversations to which one of the parties has consented. The trial judge held that the police authorities had infringed the defendant"s right to be secure from unreasonable search and seizure under section 8 of the Charter and ruled the evidence obtained inadmissible. The Crown appealed to the Ontario Court of Appeal which unanimously allowed the appeal. The defendant appealed to the Supreme Court of Canada.

2.21 The Supreme Court held that section 178.11(2)(a) of the Criminal Code did not infringe or deny the rights and freedoms guaranteed by section 8 of the Charter, but the interception of private communications by an instrumentality of the state with the consent of the originator or intended recipient of the communication, without prior judicial authorisation, did infringe the rights and freedoms guaranteed by section 8. La Forest J defined the issue thus:

> *—.The real question, as I see it, is whether our constitutional right to be secure against unreasonable search and seizure should be seen as imposing on the police the obligation to seek prior judicial authorisation before engaging in participant surveillance, or whether the police should be entirely free to determine whether circumstances justify recourse to participant surveillance and, having so determined, be allowed an unlimited discretion in defining the scope and duration of participant surveillance. This Court is accordingly, called on to decide whether the risk of warrantless surveillance may be imposed on all members of society at the sole discretion of the police. …*[15]

2.22 The court accepted that the use of electronic surveillance was a necessary tool in the fight against crime, but it was unacceptable in a free society that the agencies of the state should be able to use this technology at their sole discretion. A balance had to be struck between the privacy rights of the individual and the right of the state to intrude on that privacy in the furtherance of its responsibilities for law enforcement. Parliament had struck that balance by requiring judicial authorisation for electronic surveillance, but there was no restriction on participant surveillance. La Forest J was:

---

[15] Cited above, at 42.

—..unable to see any logic to this distinction between third party electronic surveillance and participant surveillance. The question whether unauthorized electronic surveillance of private communications violates a reasonable expectation of privacy cannot, in my view, turn on the location of the hidden microphone. Whether the microphone is hidden in the wall or concealed on the body of a participant to the conversation, the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing. As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense defined above, the unauthorized surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation on privacy."[16]

2.23 La Forest J went on:

–Our perception that we are protected against arbitrary interceptions of private communications ceases to have any real basis once it is accepted that the state is free to record private communications, without constraint, provided only that it has secured the agreement of one of the parties to the communication. Since we can never know if our listener is an informer, and since if he proves to be one, we are to be taken to be tacitly consenting to the risk that the state may be listening to and recording our conversations, we should be prepared to run this risk every time we speak."[17]

2.24 In La Forest J"s view, taken to its logical conclusion such an approach would destroy all expectations of privacy. There was no similarity between the risk that someone would listen to an individual"s words with the intention of repeating them and the risk involved when someone listened to those words while simultaneously making a permanent electronic record of them:

–These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the tattletale' but draws the line at concluding that we must also bear, as the price of choosing to speak to another

16 Cited above, at 47.
17 Cited above, at 47.

human being, the risk of having a permanent electronic recording made of our words."[18]

Application of the proposed offences to a party to the targeted activity

2.25 The first of the two questions raised at paragraph 2.14 above is whether a person who is a party to a conversation or activity which takes place inside "private premises" and who carries out an act falling within the scope of either of the proposed criminal offences should be exempt from criminal liability, or whether he should be required to obtain a warrant to authorise his actions. The first of the two offences proposed in Chapter 1 of this report is committed if an individual enters or remains on private premises as a trespasser with intent to obtain personal information. The question of whether or not the "target" had a reasonable expectation of privacy is irrelevant to the first offence. Provided the undercover officer was not present on the premises as a trespasser, his covert recording of a conversation to which he was a party on those premises would not fall within the scope of the first offence and no warrant would be required. It is difficult to envisage circumstances in which an undercover officer would be present on private premises as a trespasser and be party to a conversation there, but if such a situation arose his actions would fall within the scope of the first offence and require a warrant to avoid criminal liability.

2.26 For the purposes of the particular issue discussed here, the second offence is committed where a person uses a device with the intention of obtaining personal information relating to individuals in private premises in circumstances where those individuals would be considered to have a reasonable expectation of privacy. Unlike the first offence, the individual need not be a trespasser on the premises. The key consideration is whether or not the circumstances are such as would justify a reasonable expectation of privacy on the part of the other party to the conversation. In the case of an undercover officer who is a party to a conversation on private premises, it would depend on the particular circumstances as to whether another party to that conversation would be considered to have a reasonable expectation of privacy in respect of what was said.

2.27 The thrust of the two proposed offences is to prohibit conduct where an individual's privacy on private premises is breached, either by trespass (the first offence) or by the use of a device in circumstances where the individual would be considered to have a reasonable expectation of privacy (the second offence). We do not think that the mere fact that an individual is a participant in a conversation should automatically exempt him from criminal liability. In circumstances where the actions of a law enforcement officer would fall within the scope of either of the proposed offences, a warrant should still be required to conduct covert surveillance.

---

[18] Cited above, at 48.

Authorisation for use of device on private premises

2.28 The second question posed at paragraph 2.14 above is whether, because of the inherent intrusiveness of the conduct, *any* surreptitious use of a device on private premises for participant surveillance should require authorisation, regardless of whether it constitutes a criminal offence. We note that other jurisdictions do not take a consistent line on whether a law enforcement officer using a device in private premises while a party to a conversation requires authorisation.[19] On the one hand, it could be argued that "participant surveillance" is a lesser form of intrusion when compared with surveillance by device in circumstances where the law enforcement officer is not a party to the conversation. In the case of the former, the target has waived his right to privacy, at least vis-à-vis the other participant in the conversation, who could be expected to be able to give an account of the conversation from his recollection of what was said.

2.29 On the other hand, it could be said that the surreptitious use of a device on private premises is so privacy intrusive that such conduct should always require some form of authorisation, even if it occurs in relation to participant surveillance. We are persuaded by this latter argument. We have already recommended at paragraph 2.1 above that a warrant should be required to authorise covert surveillance involving the use of a device on private premises, whether or not that conduct would constitute one of the proposed criminal offences. While the particular circumstances of participant surveillance may merit special consideration, we do not think that they justify discarding a requirement for authorisation. We accordingly recommend that authorisation should be required in the case of participant surveillance on private premises involving the use of a device. Whether that authorisation in non-criminal participant surveillance should be by judicial warrant or internal authorisation is a matter we think best left to the internal guidelines to be prepared by each of the law enforcement agencies and approved by the proposed supervisory authority, taking account of the degree of intrusion involved.

---

[19] Under the *Surveillance Devices Act 2000* of the Northern Territory of Australia, a "party" to a conversation or activity does not include a law enforcement officer who in the course of his or her duty is using a surveillance device to record, listen to, observe or monitor the conversation or activity. Under the *Surveillance Devices Act 2004* of the Australian Commonwealth, a law enforcement officer acting in the course of his or her duties may, without warrant, use a surveillance device for any purpose involving listening to, or recording, words spoken by a person where the law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard. Where a law enforcement officer is an originator or one of the recipients of a conversation, no warrant need be obtained for such covert surveillance: section 38 of the Act. In the United Kingdom, Part II of RIPA provides a system for authorising the use of undercover officers and participant informers. Where an informer consents to the recording of a conversation with a suspect, this is treated as directed surveillance and is subject to internal authorisation by the relevant law enforcement agency concerned: sections 29 and 30 of RIPA.

Distinction between criminal and non-criminal "participant surveillance"

2.30 The authorisation required for covert surveillance on private premises under the approach we recommend in the foregoing paragraphs will be as follows:

(a) where the surveillance falls within the terms of either of the proposed offences, a warrant will be required to escape criminal liability;

(b) where the surveillance involves the use of a device on private premises but is neither within the terms of either of the proposed offences nor participant surveillance, a warrant will be required; and

(c) where the surveillance is participant surveillance, but does not fall within the terms of either of the proposed offences, authorisation must be obtained, but whether that should be by warrant or internal authorisation should be specified in the internal guidelines to be prepared by each of the law enforcement agencies and approved by the supervisory authority.

2.31 There may be circumstances in which it will be necessary to decide whether or not "participant surveillance" amounts to one of the criminal offences proposed in Chapter 1 in order to determine the level of authorisation which is required. We are conscious that this distinction may sometimes be difficult to draw, particularly in respect of the second proposed offence which hinges on whether or not the target had a reasonable expectation of privacy. As explained at paragraph 1.41, we intend that the test of whether or not an individual"s expectation of privacy is reasonable has two limbs, both of which must be satisfied. The first is whether the individual himself had an expectation of privacy and the second is whether that expectation would be considered reasonable by the "reasonable man." We have set out at paragraph 2.43 below the factors which we consider relevant in assessing whether an individual"s privacy expectation is reasonable. We acknowledge that this may be difficult to decide in practice, and for that reason recommend at paragraph 2.44 that the precise dividing line should be set out in the internal guidelines to be drawn up by each law enforcement agency in due course.

Covert surveillance by an informer or undercover agent

2.32 A further issue arises in relation to covert surveillance carried out on behalf of a law enforcement agency by an informer or undercover agent. As explained later in this Chapter, we propose that only authorised officers in government departments or law enforcement agencies should be able to apply for a warrant or (in the case of law enforcement agencies) an internal authorisation. We have recommended earlier in this Chapter that a

warrant should be required to carry out surveillance in certain specified circumstances which are particularly privacy-invasive, even though such surveillance does not amount to a criminal offence.[20] Unless provision is made to cover agents and informers, there would be a gap in the proposed scheme of control: while, for instance, a law enforcement agency would be required to obtain a warrant before conducting covert surveillance likely to involve acquisition of confidential journalistic material, no such requirement would apply to an informer who was "wired" by a law enforcement agency.[21]

2.33 Clearly, there is no distinction to be drawn in terms of the degree of intrusion on privacy between covert surveillance undertaken by an officer of a law enforcement agency and that undertaken by an informer or undercover

---

[20] See paras 2.2 to 2.13 above.

[21] In the United Kingdom, the use of undercover agents and informers is regulated under RIPA. Section 26(8) provides that a person is a "covert human intelligence source" (CHIS) if:

> *~~(~~a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything within paragraph (b) and (c);*
> *(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or*
> *(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship."*

"Directed surveillance" by a CHIS must be authorised by a designated person in one of the public authorities entitled to authorise the use or conduct of a source, as listed in Schedule 1 to RIPA. "Directed surveillance" is defined in section 26(2) of RIPA as surveillance which is covert but not intrusive and which is undertaken:

> *~~(~~a) for the purposes of a specific investigation or a specific operation;*
> *(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and*
> *(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be* sought for the carrying out of the surveillance."

Section 28(2) of RIPA provides that authorisation for directed surveillance must not be granted unless the authorising officer believes that the surveillance is both necessary and proportionate to what is sought to be achieved by carrying it out. Section 29(3) of RIPA states that an authorisation for the use of a CHIS is necessary if it is necessary:

> *—(a in the interests of national security;*
> *(b) for the purpose of preventing or detecting crime or of preventing disorder;*
> *(c) in the interests of the economic well-being of the United Kingdom;*
> *(d) in the interests of public safety;*
> *(e) for the purpose of protecting public health;*
> *(f) for the purpose of assessing or collecting any tax, duty, levy, or other imposition, contribution or charge payable to a government department; or*
> *(g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State."*

Paragraph 4.14 of the *Covert Human Intelligence Sources Code of Practice* (CHIS Code) provides that an application for authorisation for the use or conduct of a source should be in writing, stating the reasons why the authorisation is necessary and proportionate, the purpose for which the source will be tasked or deployed, the nature of what the source will be tasked to do, the details of any potential collateral intrusion and why the intrusion is justified and the details of any confidential information that is likely to be obtained.
Paragraph 4.41 of the CHIS Code provides that a source, whether or not wearing a surveillance device and invited into residential premises or a private vehicle, does not require additional authorisation to record any activity taking place therein in his presence.

agent on behalf of a law enforcement agency. We therefore think it right that similar authorisation should be required in respect of both. Where a law enforcement agency wishes to use an informer or undercover agent to undertake covert surveillance on its behalf, the agency should be required to obtain the same level of authorisation which would have been necessary if the covert surveillance in question were carried out by an officer of the law enforcement agency itself. Provision should be made to exempt an informer or undercover agent from the application of the offences proposed in Chapter 1 where the requisite authorisation has been obtained.

Use of tracking devices for covert surveillance

2.34 An issue that was not raised in the consultation paper but warrants discussion in this report is in what circumstances the use of a tracking device as a means of covert surveillance of an individual should require prior authorisation, whether by warrant or by internal authorisation. We are concerned here only with surveillance which is targeted at an individual, and not with, for instance, the use of a tracking device to monitor a consignment of goods.

2.35 A tracking device is a radio transmitter that emits a recurrent signal at a set frequency. When monitored by directional finders, the device provides information as to the location and movement of the object to which it is attached.[22] Tracking devices come in many forms. The simplest is the beeper, which emits a signal that can be traced.[23] A mobile phone can also be used as a tracking device, since its location can be determined so long as the phone is turned on. A distinction can be drawn between two types of tracking device: continuous tracking devices (such as a mobile phone when turned on) and non-continuous tracking devices (such as a credit card, personalised Octopus card, or auto toll card, which only pinpoint the location of the card at the time it is used). Arguably, continuous, or "real time", tracking is more intrusive than non-continuous tracking.

2.36 In Australia, a law enforcement officer may use a tracking device[24] without a warrant but with the written permission of an "appropriate authorising officer" [25] when investigating a relevant offence. [26] The

---

22 Clifford Fishman, *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered*, 34 Cath UL. Rev 277, at 281.

23 Other tracking devices include "over-the-horizon" radar; bistatic sensor devices, which passively pick up various types of emissions (eg from a cellular phone or a light source) or utilise an active sonar-like capability; and tagging systems, which use a projectile launcher to attach a beeper to a fleeing vehicle. See Christopher Slobogin, *Technologically-assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, Harvard Journal of Law & Technology, Volume 10, No 3 Summer 1997.

24 A tracking device is defined under section 6 of the *Surveillance Devices Act 2004* of Australia to mean any "*electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object*".

25 An "appropriate authorising officer" is a law enforcement officer holding a senior rank including that of the Commissioner or Deputy Commissioner of Police or his authorized representative, or any officer holding equivalent rank in other law enforcement agencies as specified in section 6 of the *Surveillance Devices Act 2004* of Australia.

26 Section 39(1), *Surveillance Devices Act 2004* of Australia.

authorisation may remain in force for a period not exceeding 90 days.[27] The device may be retrieved without a warrant if written authorisation is obtained.[28] However, authorisation for the use, installation or retrieval of a tracking device cannot be given if it would involve entry onto premises or interference with the interior of a vehicle without permission.[29]

2.37 In the United States, entry by the police into the interior of a vehicle without the consent of the owner to install a beeper has been held to be an intrusion for which a warrant is required.[30] A warrant is also necessary if attachment of the beeper requires trespass onto private property.[31] On the other hand, a warrant was not required where a beeper was attached to the exterior of a vehicle parked in public, as this did not constitute an invasion of privacy.[32] However, the use of a beeper to locate an item inside a particular house amounted to an intrusion for which judicial authorisation was required.[33]

2.38 In the United Kingdom, surveillance carried out by means of a device designed or adapted principally for the purpose of providing information about the location of a vehicle is regarded as "directed surveillance" for which internal authorisation from a designated officer of the public authority concerned is sufficient.[34]

2.39 After careful consideration, we have concluded that the supervisory authority should be required to decide the circumstances in which a warrant or internal authorisation should be required to allow a law enforcement agency to use a tracking device for covert surveillance of an individual.[35] In deciding the appropriate type of authorisation required, the supervisory authority should have regard to the accuracy of the tracking device used, the extent of the intrusion on the individual's privacy, and whether or not the tracking is continuous. The warrant or internal authorisation is intended to allow conduct by the law enforcement agencies which would otherwise fall within one of the proposed surveillance offences.

2.40 The grounds and procedures for the application for a warrant or internal authorisation for covert surveillance (including those recommended for emergency situations) set out in this report should be applicable to an

---

27 Section 39(7), *Surveillance Devices Act 2004* of Australia.

28 Section 39(6), *Surveillance Devices Act 2004* of Australia.

29 Section 39(8), *Surveillance Devices Act 2004* of Australia.

30 *Butts* 710 F.2d at 1147; *Hufford* 539 F.2d at 34; *United States v Cofer* 444 F Supp 146, 149; *People v Smith* 67 Cal App 3d 638, 654.

31 *Hufford* 539 F 2d at 34, see also *United States v Rowland* 448 F Supp 22.

32 In *United States v Knotts* 460 US 276 (1983), at 282, the US Supreme Court held that using a beeper to track a car through public streets was not a search under the Fourth Amendment. According to the Court, it was not reasonable to expect privacy with respect to one's route or destination when travelling on the roadways.

33 *United States v Karo* 468 US 705 (1984). The warrant need not state with particularity the place to be searched by the beeper when that place is unknown.

34 Section 26(4), *Regulation of Investigatory Powers Act 2000*. See also Michael Cousens, *Surveillance Law*, Chapter 8, para 8.9.

35 Chapter 8 describes in detail the composition and functions of the proposed supervisory authority.

application for a warrant or internal authorisation for the use of a tracking device.

Circumstances in which internal authorisation is required to conduct covert surveillance

2.41 We take the view that legal control should extend to situations where a person‟s reasonable expectation of privacy is intruded on by the covert surveillance of law enforcement agencies. In this respect we endorse the following views expressed in the Commission‟s report on *Civil Liability for Invasion of Privacy*:

> *—We admit that a person‘s reasonable expectation of privacy is considerably less when he is in a public place than when he is at home, and the taking of casual photographs in a public place should not normally be held to be an invasion of the privacy of a person who happens to be captured by such a photograph. However, a person does not forfeit all legitimate expectation of privacy when he ventures to a public place or a place to which the public has access. The fact that the plaintiff is in a private or public place is not conclusive in determining whether he has a reasonable expectation of privacy. Targeted photography or filming of a person inside a gymnasium, public toilet, methadone clinic, job centre, funeral parlour, church, hospital ward or waiting area of a social hygiene clinic, is intrusive if done without that person‘s consent – even though he is in a place accessible to the public. These places are in a sense public but where people expect a reasonable degree of seclusion. Another example is the use of an electronic listening advice to spy on another person‘s conversation from a distance. It intrudes upon the privacy of the interlocutors whether the conversation is conducted in a public place or not.*
>
> *We also agree with the observation that the mere fact that a person can be seen by others does not mean that he cannot be secluded in a legal sense. Seclusion need not be absolute. He can be visible to some people without forfeiting his right to remain secluded from others. The fact that the privacy one expects in a given setting is limited and is not complete should not render the expectation unreasonable as a matter of law.”*[36]

2.42 We recommend that internal authorisation must be obtained from a designated senior officer of the law enforcement agency where covert surveillance is to be carried out for a specific investigation or operation in circumstances in which a person is likely to have a reasonable expectation of

[36] Law Reform Commission report on *Civil Liability for Invasion of Privacy*, paras 6.41 and 6.42.

privacy, even though the act does not involve intrusion of a sort that requires a warrant.[37]

2.43 However, we accept that privacy is a matter of degree. It would not be possible to set out in the legislation all the circumstances in which a person would be entitled to a reasonable expectation of privacy. In assessing whether an individual"s privacy expectation is reasonable, we believe that the following factors are relevant:

(a) **the place where the intrusion occurred** (eg, whether the individual is at home, in office premises or in a public place, and whether or not the place is open to public view from a place accessible to the public, or, as the case may be, whether or not the conversation is audible to passers-by);

(b) **the object and occasion of the intrusion** (eg, whether it interferes with the intimate or private life of the individual);

(c) **the means of intrusion employed and the nature of any device used** (eg, whether the intrusion is effected by means of a high-technology sense-enhancing device, or by mere observation or natural hearing); and

(d) **the conduct of the individual prior to or at the time of the intrusion** (eg, whether it amounts to a waiver, in whole or in part, of privacy in respect of the intrusion, such as by actively inviting interest in his private life or voluntarily releasing intimate information about himself, and whether the individual has taken any steps to protect his privacy).

2.44 We recommend that the legislation should require each law enforcement agency to issue internal guidelines specifying the factors that should be taken into account by its officers in an application for, and in the grant of, internal authorisation for covert surveillance. The guidelines must be approved by the supervisory authority before they are applied by a law enforcement agency, and the guidelines should be made available to the public.

---

[37] In *Campbell v MGN Ltd* [2004] 2 AC 457, [2004] 2 All ER 995. the issue was whether there had been wrongful disclosure of private information. The House of Lords, by a majority of three to two, held that the details of the plaintiff"s treatment with Narcotics Anonymous, together with the photographs, constituted private information the publication of which amounted to a breach of confidence. Lord Hope accepted that a duty of confidence will arise whenever the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected. See footnote 17 of Chapter 1 of this report.

Application by the private sector

Recommendations in the consultation paper

2.45 In the consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*, the sub-committee took the view that in some situations private agencies might be able to show that their intended surveillance activities would further one of the public interests justifying intrusion, such as the prevention or detection of serious crime. The sub-committee therefore recommended 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."*[38]

The responses to the consultation paper

2.46 A number of respondents objected to the proposal to allow private parties to apply for a warrant to conduct covert surveillance, on the grounds that they would not be subject to any licensing regulations or disciplinary measures.

Revised recommendations

2.47 Having reviewed the recommendations in the consultation paper in the light of the response, we have concluded that the power to conduct covert surveillance should lie solely in the hands of the Administration, which is entrusted with the responsibility to maintain law and order and is accountable to the public.

2.48 If the private sector were allowed to conduct covert surveillance, it would be extremely difficult to control the subsequent use and disclosure of information obtained through such means. There is no guarantee that the power to conduct covert surveillance would be exercised in a proper manner where such conduct was undertaken by a private individual or organisation. We believe the potential for abuse outweighs any advantage in allowing the private sector to apply for warrants to conduct surveillance.

2.49 We therefore recommend that the right to apply for a warrant should be restricted to the Administration and its law enforcement agencies.

---

[38] Consultation paper, para 6.21.

Who may apply for a warrant to conduct covert surveillance

2.50 Where a warrant authorising covert surveillance is required before such conduct can be carried out lawfully for law enforcement purposes, we recommend that an authorised officer of any department of the Government of the Hong Kong Special Administrative Region, or of the Independent Commission Against Corruption, should be permitted to apply to the Court of First Instance for a warrant authorising covert surveillance to be carried out by officers of that department.

2.51 We recommend that any application for a warrant for covert surveillance by a department other than the Hong Kong Police Force, the Customs and Excise Department, the Immigration Department and the Correctional Services Department must be made on that department‟s behalf by the Department of Justice. This is to ensure that any warrant application made to the Court of First Instance would *prima facie* satisfy the requirements for the issue of a warrant and that there are merits in the application.

Who may apply for internal authorisation

2.52 We further recommend that in cases where internal authorisation is legally sufficient to enable covert surveillance to be carried out for law enforcement purposes, an application for internal authorisation to carry out such covert surveillance may only be made by designated officers of the Independent Commission Against Corruption or any of the following Government departments:

(a) the Hong Kong Police Force;

(b) the Customs and Excise Service;

(c) the Immigration Department; or

(d) the Correctional Services Department.

2.53 In reaching the view that the power to issue internal authorisations should only be accorded to the five designated agencies, we have taken into account the fact that the use of such covert and intrusive means of law enforcement should only be given to disciplined law enforcement bodies which have adequate internal supervision and which possess sufficient technical experience.[39]

[39] This recommendation is in line with the Executive Order No 1 of 2005, under which an application for authorisation for covert surveillance can only be made and granted by "*a department of the Government which as part of its functions, undertakes law enforcement investigations or operations*" and by the Independent Commission Against Corruption. See sections 2 and 5 of the Executive Order.

Chapter 3

Grounds for the issue of warrants and internal authorisations for covert surveillance

---

Grounds for the issue of warrants

Recommendations in the consultation paper

3.1 In its consultation paper, the sub-committee recommended the issue of a warrant authorising surveillance should only be justified on public interest grounds, namely, for the purpose of preventing or detecting serious crime, or where surveillance was likely to be of substantial value in furthering security, defence, or international relations in respect of Hong Kong.[1]

Review of previous recommendations

3.2 We have reviewed the recommendations in the consultation paper, and now recommend that the grounds for issuing a warrant authorising covert surveillance should be that:

(a) it is for the purpose of preventing or detecting serious crime; or

(b) it is for the purpose of safeguarding public security in respect of Hong Kong.

Prevention and detection of serious crime

Review of meaning of "serious crime"

3.3 Our guiding principle is that the means of investigation should be proportionate to the gravity of the matter under investigation. The consultation paper recommended that an offence punishable by a maximum sentence of at least seven years imprisonment should be classified as "serious crime" as this would adequately reflect the gravity of the offence that justifies the issue of a warrant. The consultation paper further recommended that "serious crime" should also include an offence punishable by a maximum sentence of at least three years imprisonment where there was an element of bribery or corruption. This was to reflect the fact that those offences may still

---

[1] Paras 6.41 and 6.50, consultation paper.

be considered as posing such a threat to society that they should fall within the scope of "serious crime" for the purposes of the warrant proposal.[2]

3.4 An alternative of adopting a schedule of offences which constituted "serious crimes" was proposed by some respondents to the consultation paper. This is the approach adopted in Canada[3] and the United States,[4] where offences which may form the basis of an application for an authorisation to intercept communications are listed in a schedule to the relevant legislation. Such an approach would require constant updating and revision, however, and for that reason we reject the proposal.

3.5 The Bar Association objected to the proposal to define "serious crime" by reference only to the maximum sentence, without regard to the circumstances of each case. We believe that defining "serious crime" by virtue of the maximum sentence achieves the necessary certainty in the law and avoids the difficulty of listing each offence separately. In Australia, authorisation may be granted for surveillance for investigation of "relevant offences".[5] In the United Kingdom, intrusive surveillance may be conducted for the purpose of preventing or detecting "serious crime".[6]

3.6 Having taken into account the responses to the consultation paper and the approaches followed in other jurisdictions, we maintain the view that "serious crime" should be defined by reference to the maximum sentence applicable to the offence. We believe that an offence should be considered a "serious crime" if it is punishable by imprisonment for a maximum period of at least seven years, but we accept that the determination of the appropriate level of sentence should be a matter for the Administration. We recommend that the Administration should be able to include in addition in a schedule to the proposed legislation those offences which do not meet the requisite level of sentence but which may still be so harmful to the community that they should be classified as "serious crimes" for surveillance purposes.

Review of meaning of "prevention and detection" of serious crime

3.7 The consultation paper's definition of "prevention and detection" of crime did not extend to the prosecution of the offence. Intrusions were to be lawful up to, but not including, the prosecution of an offence, with the cut-off point between prevention / detection and prosecution being the laying of the charge.[7]

---

2 Para 6.36, consultation paper.

3 Section 183, Canadian *Criminal Code*.

4 Section 2516, US *Wiretap Act*.

5 Sections 6 and 14, *Surveillance Devices Act 2004* of Australia. "Relevant offence" is defined to include generally an offence punishable by a maximum term of imprisonment of three years or more or for life and certain prescribed offences.

6 Sections 32(2)(b) and 81(3), UK *Regulation of Investigatory Powers Act 2000*. An offence that could result in imprisonment for a term of three years or more may constitute a "serious crime".

7 Paras 6.37 to 6.40, consultation paper. This interpretation followed the decision of the House of Lords in *R v Preston* [1993] 4 All ER 638 where Lord Mustill stated that prevention and detection in terms of the Interception of Communications Act 1985, s2(2)(b), did not include the prosecution of crime: "*to my mind the expression 'preventing and detecting' calls up only two*

3.8 In view of the revised recommendation in Chapter 5 of this report that evidence obtained by covert surveillance should be admissible in legal proceedings, subject to a judicial discretion to exclude evidence that would prejudice a fair trial, we propose to extend the scope of the meaning of the "prevention and detection" of crime to include the prosecution of an offence.[8]

Safeguarding public security in respect of Hong Kong

3.9 The consultation paper recommended that a further ground for issuing a warrant authorising covert surveillance should be "where [intrusions] 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".[9]

3.10 In its report on *Privacy: Regulating the Interception of Communications,* the Law Reform Commission expressed reservations as to the certainty with which the boundaries of "international relations" could be delineated. The Commission further noted that Article 30 of the Basic Law provides that the only ground on which a resident's privacy of communication may be infringed is "public security" or "investigation into criminal offences". The Commission took the view that, although the term "public security" had not been defined, it would be wide enough to cover defence and, in certain circumstances, international relations. The Commission therefore recommended that, instead of a reference to "security, defence or international relations", the relevant ground for issuing a warrant should be restricted to "public security in respect of Hong Kong."[10]

3.11 On further considering these points, we take the view that the term "public security" is wide enough to cover defence and, in certain circumstances, international relations.[11] We have accordingly decided to modify the recommendation in the consultation paper: instead of a reference to *"security, defence or international relations",* this ground for a warrant should be restricted to *"public security in respect of Hong Kong*".[12]

---

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 ends."

8 Section 81(5) of the *Regulation of Investigatory Powers Act 2000* has extended the definition of detecting crime to include: (a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and (b) the apprehension of the person by whom any crime was committed.

9 Para 6.50, consultation paper.

10 Paras 6.63 to 6.64, report on *Privacy: Regulating the Interception of Communications*.

11 Section 3 of the Executive Order No 1 of 2005 provides that one of the purposes for authorising covert surveillance is for "*protecting public safety or security*". We take the view that "public security" already includes the idea of "public safety". We therefore reject the protection of "public safety" as an additional ground for application or for the grant of a warrant or an internal authorisation for covert surveillance.

12 In *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, the House of Lords made the following observation on the meaning of "national security": "*The question of whether something is 'in the interests' of national security is not a question of law. It is a matter of judgment and policy. Under the constitution of the UK and most other countries, decisions as*

Safeguarding the stability of Hong Kong's financial system

3.12 The consultation paper recommended that one of the grounds for issuing a warrant should be that it was for the purpose of safeguarding the stability of the local financial system, and this should extend to intrusions conducted both within and outside Hong Kong.[13] The majority of those responding to the consultation paper objected to this proposal. Upon review, we conclude that neither the stability of the local financial system nor the economic well-being of Hong Kong is a matter of such gravity as to justify the issue of warrants for covert surveillance unless the threat to the financial system or economic well-being impinges on the public security of Hong Kong.

Matters on which the court must be satisfied

General principles

3.13 The grounds on which the court must be satisfied before authorising the use of covert surveillance should reflect the requirements for the protection of an individual's right to privacy guaranteed under Articles 29 and 30 of the Basic Law, and Article 17 of the International Covenant on Civil and Political Rights as incorporated in Article 14 of the Hong Kong Bill of Rights.

3.14 Judicial authorisation provides prior independent scrutiny to ensure that interference with the privacy rights of an individual is necessary to achieve legitimate aims and that the means employed are proportionate to those legitimate aims.

3.15 In deciding whether to grant an application for a warrant to carry out covert surveillance, the court should satisfy itself that the proposed intrusion is for a legitimate purpose. The court should ensure that the means of investigation are proportionate to the immediacy and gravity of the alleged offence. The court should balance the need for the covert surveillance in operational terms against the intrusiveness of the activity on the target and on others who may be affected by it. There must be reasonable suspicion that the individuals to be subject to covert surveillance are involved in the commission of a serious crime. In addition, the court must be satisfied that information relevant to the purpose of the covert surveillance is likely to be obtained and that such information cannot reasonably be acquired by less intrusive means.[14]

---

to whether something is in the interests of national security are not a matter for judicial decision. They are entrusted to the executive."

13 Para 6.54, consultation paper.

14 Similar requirements can be found under section 32(2) of the United Kingdom's *Regulation of Investigatory Powers Act 2000* with regard to intrusive surveillance: *"(2) Neither the Secretary of State nor any senior authorising officer shall grant an authorisation for the carrying out of intrusive surveillance unless he believes – (a) that the authorisation is necessary on grounds falling within subsection (3); and (b) that the authorised surveillance is proportionate to what is*

Recommendations

3.16 We accordingly recommend that a warrant authorising covert surveillance may be issued if the judge is satisfied that:

(a) the covert surveillance is to be carried out for a legitimate purpose, namely, for the purpose of preventing or detecting serious crime, or for protecting public security in respect of Hong Kong;

(b) the covert surveillance is proportionate to what is sought to be achieved by carrying it out.

In deciding whether the covert surveillance is proportionate to the purpose sought to be achieved by carrying it out, the court must be satisfied that:

(a) there is reasonable suspicion that an individual is committing, has committed, or is about to commit, a serious crime or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong;

(b) there is reasonable belief that information relevant to the investigation will be obtained through the covert surveillance; and

(c) the information to be obtained cannot reasonably be obtained by less intrusive means;

3.17 In reaching its decision, the court should have regard to the following factors:

---

sought to be achieved by carrying it out.(3)… an authorisation is necessary on grounds falling within this subsection if it is necessary y- (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; or (c) in the interests of the economic well-being of the United Kingdom …. (4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means." The *Covert Surveillance: Code of Practice* further explains at paras 2.4 to 2.5 that: *—Obtaining an authorisation under the 2000 Act … will only ensure that there is a justifiable interference with an individual's Article 8 rights [rights to privacy under the European Convention of Human Rights] if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 28(3) of the 2000 Act for directed surveillance and in section 32(3) of the 2000 Act for intrusive surveillance. Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair."*

(a) the immediacy and gravity of the serious crime or the threat to public security in respect of Hong Kong, as the case may be;

(b) the place where the intrusion will occur;

(c) the means of intrusion to be employed and the nature of any device to be used; and

(d) taking into account any reasonable expectation of privacy in the circumstances, the extent to which the privacy of the individual subject to the covert surveillance and of any other person may be affected by the surveillance.

Grounds for the issue of internal authorisations

General principles

3.18 The general principles governing the issue of internal authorisations for covert surveillance are similar to those regulating the grant of warrants by the court.

Recommendations

3.19 We recommend that an internal authorisation to undertake covert surveillance may be issued if the authorising officer is satisfied that:

(a) the covert surveillance is to be carried out for a legitimate purpose, namely, for the purpose of preventing or detecting crime, or for protecting public security in respect of Hong Kong;

(b) the covert surveillance is proportionate to what is sought to be achieved by carrying it out.[15]

3.20 The reference in condition (a) to the prevention or detection of "crime" (rather than "serious crime" as in the case of a warrant) is to provide greater flexibility to the law enforcement agencies in the investigation of offences in circumstances where the use of covert surveillance would have a

[15] A similar test for issue of authorisation and renewal of covert surveillance is found in section 3 of the Executive Order No 1 of 2005. Section 3 reads*: –In this Order, the conditions for the grant of an authorization for covert surveillance, or a renewal of an authorization for covert surveillance, are that, in the circumstances of the particular case – (a) the purpose sought to be furthered by carrying out the covert surveillance is that of - (i) preventing or detecting crime; or (ii) protecting public safety or security; and (b) the covert surveillance is proportionate to the purpose sought to be furthered by carrying out it out, upon - (i) balancing, in operational terms, the need for the covert surveillance against the intrusiveness of the covert surveillance on any person who is to be the subject of or may be affected by the covert surveillance; and (ii) considering whether the purpose sought to be furthered by carrying out the covert surveillance can reasonably be furthered by other less intrusive means."*

less intrusive effect on the individual's right to privacy than those under which judicial authorisation is required.

Matters to be taken into account in assessing proportionality

3.21 In deciding whether the covert surveillance is proportionate to the purpose sought to be achieved, the authorising officer must be satisfied that:

(a) there is reasonable suspicion that an individual is committing, has committed or is about to commit a crime, or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong;

(b) there is reasonable belief that information relevant to the investigation will be obtained through the covert surveillance; and

(c) the information to be obtained cannot reasonably be obtained by less intrusive means;

3.22 In reaching his decision, the authorising officer 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 place where the intrusion will occur;

(c) the means of intrusion to be employed and the nature of any device to be used; and

(d) taking account of any reasonable expectation of privacy in the circumstances, the extent to which the privacy of the individual subject to the covert surveillance and any other person may be affected by the surveillance.

Disclosure of surveillance materials

3.23 In respect of both warrants and internal authorisations, the judge or authorising officer must make appropriate arrangements to ensure that the disclosure of surveillance materials is limited to the minimum necessary. We consider this point later in Chapter 6.

Chapter 4

The procedure for authorisation

The issuing authority

Warrants

4.1 We maintain the recommendation in the consultation paper that all applications for warrants for covert surveillance should be made to a judge of the Court of First Instance. A limited number of judges should be appointed by the Chief Executive on the recommendation of the Chief Justice for a fixed term to deal with applications for warrants. Having a limited number of judges would be conducive to developing expertise and broad consistency of approach. Further, this arrangement is necessary since the judges dealing with applications for warrants would not be able to hear cases arising out of the applications or the investigations for which they were made. It would be necessary to provide the Judiciary with sufficient additional resources to deal with applications for warrants.

Internal authorisations

4.2 We recommend that internal authorisations for covert surveillance should be issued by an officer equivalent to at least the rank of Senior Superintendent of Police in the law enforcement agency concerned. We note that this approach is similar to that adopted in the Chief Executive"s Order No 1 of 2005, which refers to an officer at the top of the Master Pay Scale.

Information to be provided in an application for a warrant or internal authorisation for covert surveillance

4.3 The consultation paper made no detailed recommendations on the information to be provided in an application for a warrant authorising surveillance. In our view, if the court or authorising officer is to make an informed decision as to whether or not to grant an application, it is essential that the law enforcement officer provide sufficient information to show that covert surveillance is necessary for the intended purpose.

4.4 We recommend that an application for a warrant or an internal authorisation to undertake covert surveillance should be in writing[1] and should include the following information:

(a) the name and rank or post of the person making the application;

(b) the ground(s) upon which a warrant or internal authorisation is sought;

(c) the facts relied upon to justify the belief that a warrant or internal authorisation should be issued, including the particulars of the crime, including serious crime under investigation, or the threat to public security in respect of Hong Kong;

(d) the identity of the individual(s), if known, who is or are to be the subject of the covert surveillance;

(e) the information sought through covert surveillance;

(f) the form of covert surveillance and the kind of surveillance device(s) to be used;

(g) the location of the facilities from which, or the place where, the covert surveillance is to be carried out;

(h) the number of instances, if any, on which an application for a warrant or internal authorisation has been made in relation to the same subject matter or the same person and whether that previous application was rejected or withdrawn;

(i) the period for which the warrant or authorisation is requested;

(j) whether the covert surveillance is likely to result in any person acquiring knowledge of matters subject to legal privilege, confidential journalistic information or sensitive personal information;

(k) the details of any potential collateral intrusion and why the intrusion is justified;

(l) whether other less intrusive means have been tried and why they have failed or are unlikely to succeed;

(m) the reasons why the covert surveillance is considered proportionate to what it seeks to achieve; and

[1] It is not necessary to make separate provision for telephone or oral applications in emergency situations as the law enforcement officer is required to provide the court or the authorising officer with full particulars in writing in support of the application within 24 hours of the application.

(n) the extent to which, and the number of persons to whom, any material obtained by covert surveillance is likely to be disclosed; the extent to which the surveillance material will be copied and the estimated number of copies likely to be made of any of the surveillance material obtained.[2]

Duration and renewal of authorisation

Recommendations in the consultation paper

4.5 The consultation paper recommended that a warrant for surveillance should be issued for an initial period of 60 days. The paper recommended that renewals might be granted for such further periods of the same duration as were shown to be necessary. The paper further recommended that there should be no upper limit to the number of extensions given.[3]

Review of previous recommendations

Initial application

4.6 We have reconsidered this recommendation, and now recommend that a warrant for covert surveillance may be granted by the Court of First Instance for an initial period not exceeding 90 days.[4] We recommend that an initial internal authorisation may be issued by a designated authorising officer of the law enforcement agency concerned for the same duration.[5]

Application for renewal

4.7 In respect of an application for renewal of an internal authorisation, we recommend that this should be made on the first occasion to

---

2 The purpose of item (n) is to ensure that the court or the authorising officer is provided with sufficient information to ensure that the disclosure of surveillance materials is limited to a necessary minimum when granting a warrant or internal authorisation for covert surveillance. See para 6.66 of Chapter 6.

3 Paras 6.55 - 6.56, consultation paper.

4 It is noted that a warrant may be issued for a period not exceeding 90 days under section 6(4) of the *Interception of Communications Ordinance* (Cap 532). Similar recommendations have been made in the Law Reform Commission report on *Privacy: Regulating the Interception of Communications*, paras 6.125 – 6.127. Section 8 of the Executive Order No 1 of 2005 provides that the duration of authorisation shall not be longer than a period of three months from the time when it takes effect.

5 Under the US *Wiretap Act*, section 2518(5), wiretapping cannot last for longer than is necessary to achieve the objective of the authorisation, nor in any event longer than 30 days. Sections 17 and 19 of the Australian *Surveillance Devices Act 2004* provide that the maximum duration of a surveillance device warrant is 90 days and may be extended for up to 90 days. There is no limit to the number of extensions that can be made. Under the UK *Regulation of Investigatory Powers Act 2000*, section 43(3)(c), *Covert Surveillance: Code of Practice*, para 4.19, the duration of authorisation in respect of both directed and intrusive surveillance is three months.

the appropriate approving officer in the law enforcement agency concerned. An application for a second or subsequent renewal of an internal authorisation should be made to the Court of First Instance before its expiration, as should any application for renewal of a warrant. A renewal should only be granted in respect of the same subject matter as the previous application for a warrant or authorisation.

4.8 A warrant or an authorisation may be renewed for a further period not exceeding 90 days if the court (or the approving officer, as the case may be) is satisfied that the grounds on which the warrant or internal authorisation was issued still exist. We agree with the consultation paper's recommendation that there should not be any limit to the number of renewals that can be made.

4.9 An application to the court for renewal of a warrant or an internal authorisation may be made *ex parte.* It should be in writing and should include the following information:

(a) the reason and period for which the renewal is required;

(b) the type of information likely to be obtained from surveillance;

(c) the particulars of any previous applications involving the same person; and

(d) the reasons why the covert surveillance continues to be considered proportionate to what it seeks to achieve.

In respect of point (d), where circumstances have changed, the law enforcement agency would need to explain those changes and give reasons why the use of covert surveillance should still be considered proportionate.

Detailed procedures

4.10 We recommend that detailed procedures governing the application for, and the renewal of, warrants should be specified in legislation. There should be a statutory requirement that internal guidelines regulating procedures for application and renewal of internal authorisations be issued by the relevant law enforcement agencies. Those guidelines should be subject to approval by the supervisory authority. The internal guidelines should be made available to the public.

Emergency application for a warrant or internal authorisation

Recommendations in the consultation paper

4.11 The consultation paper recommended that where it was impractical because of the urgency of the situation (such as where life was at

risk) to obtain approval from the court before initiating surveillance, it should be permissible to apply to the court *ex post facto* for a warrant.[6] This proposal was generally supported by those who responded to the consultation paper.[7]

Review of previous recommendations

4.12 Clearly, circumstances may arise in which covert surveillance is required but the urgency of the situation means that it would not be practicable to apply for a warrant or authorisation in the usual way. There may, for instance, be a situation where important evidence could be obtained by surveillance but there is a serious risk that that evidence will be lost unless surveillance is undertaken immediately. The consultation paper proposed that such circumstances should be met by allowing for *ex post facto* application to be made for a warrant or internal authorisation. An alternative approach would be to devise a procedure which would allow emergency applications to be made orally by telephone or other electronic means. The attraction of such an approach is that it ensures that there is some oversight (albeit in a reduced form) before surveillance is undertaken, rather than leaving authorisation until after the emergency surveillance has begun.

4.13 We are attracted to the option of providing a procedure for emergency applications, but we consider that there may still be circumstances where the subsequent ratification of the surveillance process by means of *ex post facto* application will be necessary. We recommend in such circumstances that a law enforcement officer should be able to authorise covert surveillance for an initial 24 hour period. A judge would then have to consider whether the authorisation should have been granted in the first place, and whether it should be continued. Alternatively, where circumstances permit, a prospective emergency application may be made for authorisation of covert surveillance, in the manner described below. Given the availability of a procedure for emergency application, we would expect the circumstances in which *ex post facto* authorisation would be necessary to be exceptional. An example of such circumstances might be where an undercover officer learns at short notice of a meeting of conspirators at which he is to be a participant, but cannot absent himself in advance of the meeting to contact his superiors for authorisation without arousing the conspirators" suspicions.

The mode of emergency application

4.14 The emergency procedure would only apply in serious situations where there was either an urgent threat or an urgent need to conduct

---

6 Para 6.20, consultation paper.

7 Only one respondent, the Hong Kong Alliance of Chinese and Expatriates, objected to the idea of allowing a person to apply for retrospective judicial authorisation. It took the view that applications should be made to the duty judge, even in cases of emergency, through some form of informal authorisation such as telephone requests or disposition pending proper documentation.

surveillance to avoid losing critical information.[8] In such circumstances, we recommend that an application for a warrant may either be made orally by telephone or by a law enforcement officer appearing in person before the court or by other electronic means, including facsimile and e-mail. We do not think that such a requirement is likely to adversely affect the operational efficiency of the law enforcement agencies since the duty judge system provides 24 hours access to the Court of First Instance for consideration of such applications.

4.15 In respect of an application for an internal authorisation, an emergency application may be made in oral form or by electronic means of communication to an officer of the rank of Assistant Commissioner of Police or its equivalent in the relevant law enforcement agency. In respect of both warrants and internal authorisations, the emergency authorisation would be valid for only 24 hours, and a full application providing details of the reason and grounds for the emergency authorisation would have to be submitted in writing within 24 hours of the original emergency application to the court or to the appropriate authorising authority. Where the need for further information arises, the court or the authorising authority may require the personal appearance of the law enforcement officer making the urgent application and may impose conditions on the execution of the warrant or the internal authorisation.

4.16 We think it right to allow emergency applications to be made orally, given that technological developments now mean that the oral transmission of emergency applications is feasible.

The grounds for an emergency application

4.17 We recommend that an application for emergency authorisation may be made to the court or an authorising officer if a law enforcement officer reasonably believes that:

(a) the circumstances are so serious and urgent that covert surveillance should be used; and

(b) it is not practicable to apply for a warrant or authorisation in the usual way.

4.18 The emergency application may be granted if the court or the authorising officer is satisfied that there are reasonable grounds to believe that the two conditions specified in items (a) and (b) above exist and that the criteria for granting a warrant or an authorisation under normal circumstances have been fulfilled.[9] We should stress that an application for the renewal of a

---

[8] Examples of what may constitute "serious and urgent" threat for the purposes of this proposed provision for emergency application for authorisation include situations involving imminent threat of death or bodily harm to a person, or of substantial damage to property, or where there is a threat to public security.

[9] See chapter 3 of this report.

warrant or authorisation, regardless of the mode of application for the original warrant or authorisation, cannot be made by the emergency process. In this respect, we note that our approach differs from that adopted in the Chief Executive"s Order, which allows both the initial emergency application and its renewal to be made orally.[10]

Record of warrants and internal authorisations

4.19 We recommend that a record of all warrants and internal authorisations granted in respect of covert surveillance carried out by each law enforcement agency should be kept by that agency and regularly updated whenever a warrant or authorisation has been granted, renewed or cancelled. We leave it to the Administration to specify an appropriate minimum period for which these records should be retained from the expiry or termination of the warrant or authorisation. The keeping of such records would facilitate review by the supervisory authority of the issue of warrants and authorisations.

4.20 The records of warrants and authorisations should contain the following information:

(a) the date of the issue, expiry or termination of the warrant or authorisation;

(b) the name and rank of the authorising officer;

(c) a brief description of the investigation or operation, including names and relevant particulars of the subject(s) of the covert surveillance, if known;

(d) whether it was an emergency application, and if so, the justifications; and

(e) if the warrant or authorisation is renewed, when it was renewed and who granted the renewal;

4.21 We further recommend that each law enforcement agency should be required to keep the following documentation relating to its warrants or authorisations for surveillance:

(a) a copy of the application and a copy of the warrant or authorisation;

---

[10] Section 13 of the Executive Order provides that an application for authorisation for covert surveillance or for its renewal may be made orally if the officer making the application considers that the particular case is of such urgency as to justify the making of such an oral application. The authorising officer may grant the authorisation or renewal sought if he is satisfied that the particular case is of such urgency as to justify the making of the oral application. The authorisation or renewal granted under such oral application shall cease to have effect upon the expiration of the period specified by the authorising officer and in any case shall not be longer than the period of 72 hours beginning with the time when the authorisation or renewal takes effect.

(b) a record of the result of each review of the warrant or authorisation; and

(c) a copy of any renewal of authorisation, together with the supporting documentation submitted when the renewal was requested.

Chapter 5

Admissibility as evidence of materials obtained from covert surveillance

5.1 The question of whether or not materials obtained from covert surveillance should be admissible as evidence has a direct bearing on the circumstances in which such materials should be retained or destroyed. If surveillance materials are admissible, then the need to ensure proper disclosure to the defence will require that provision is made for the retention of such material, but such constraints will not apply if the material is uniformly treated as inadmissible. This Chapter examines the question of admissibility, while Chapter 6 looks at the retention and destruction of surveillance materials.

5.2 While the present report is concerned with covert surveillance, the same questions of admissibility arise in relation to materials obtained through the interception of communications. Notwithstanding its principal focus, it would be unrealistic for this report to refer only to the admissibility of covert surveillance materials without reference to the closely related issue of materials obtained through the interception of communications.

5.3 In its consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*, the Privacy Sub-committee recommended that materials obtained through both interception of communications and surveillance should be inadmissible as evidence, regardless of their relevance. The prohibition on use was to cover not only the fruits of interception or surveillance but also details of the methods used. The materials should be destroyed once an investigation moved into the prosecution phase. While the consultation paper recommended the same treatment for both types of material, that is not the only option. Provided a valid case can be made for distinguishing between the two classes of material, the decision on the admissibility of materials obtained through surveillance need not necessarily be the same as that adopted in respect of materials obtained through the interception of communications.

5.4 This Chapter begins with an examination of the distinction between interception of communications and covert surveillance, before setting out relevant background information in respect of the discussions held, and decisions taken, over recent years in relation to the issue of admissibility in Hong Kong and the United Kingdom. Finally, the Chapter reviews the options for the admissibility of covert surveillance materials.

The distinction between "interception of communications" and "covert surveillance"

United Kingdom provisions

5.5 Section 1(1) of the *Regulation of Investigatory Powers Act 2000* (RIPA) provides that it is an offence for a person to intercept at any place in the United Kingdom:

> *—… any communication in the course of its transmission by means of –*
>
> *(a) a public postal service; or*
>
> *(b) a public telecommunication system."*

Section 2(2) of RIPA provides that for the purposes of the Act:

> *—… a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he -*
>
> *(a) so modifies or interferes with the system, or its operation,*
> *(b) so monitors transmissions made by means of the system, or*
> *(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,*
>
> *as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."*

5.6 A "telecommunication system" is defined under section 2(1) of RIPA to mean:

> *—any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy".* [1]

5.7 The definition makes it clear that the Act is only concerned with interceptions in the course of transmission. As explained by the Government minister during the passage of the Bill through the House of Lords:

---

[1] The definition makes it clear mobile phones, emails and pagers are included: see *Surveillance Law* Michael Cousens, at para 6.36.

–The course of transmission begins where a postal service or telecommunications system first begins to transmit a communication. In a telephone, the sound waves from the human voice first begin to be in the course of their transmission by means of a telecommunication when they are received by the microphone in the handset. They continue to be in the course of their transmission until they are emitted by the speaker.

Such phraseology ensures that one is not technically intercepting a communication if one is in the same room as someone using a telephone and one happens to overhear what is being said. In the same way, listening to a voice from a speakerphone is not interception: the sound waves have left the telecommunication system on which they were transmitted, and are hence no longer technically in the course of their transmission. That is what we have in mind and why we have used that phraseology."[2]

Hong Kong provisions

The Interception of Communications Ordinance (Cap 532)

5.8 Section 2 of the Interception of Communications Ordinance (Cap 532) defines "communication" as "postal or telecommunication". "Intercept" means:

> *—theaural or other acquisition of the contents of any postal communication, telecommunication, or telecommunication through the use of any electro-magnetic, acoustic, mechanical or other device".*

5.9 "Intercepted material" is defined under section 2 of the Ordinance to mean "the contents of any postal communication or telecommunication that has been obtained through interception".

The Telecommunications Ordinance (Cap 106)

5.10 "Telecommunication" is defined in section 2 of the *Telecommunications Ordinance* (Cap 106) to mean:

---

[2] 613 HL Official Report col 1435, 12 June 2000, per Lord Bassam. There are circumstances in which it may prove difficult to draw the line between when a communication is, or is not, still in transmission. For instance, is an email which is held on a server still in transmission? And what of a voicemail message to a phone? This point appears to have been picked up by section 2(7) of RIPA, which provides that: "*For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.*"

"any transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye".

5.11 Although interception of communications may involve interception of postal mail and telecommunications[3] , the present paper is concerned only with the interception of telecommunications and "intercepted materials" in the context of this paper refers to "intercepted telecommunications material".

The case of R v E

5.12 In *R v E*[4] (an English Court of Appeal case), the police, in the course of an investigation into suspected drug dealing, placed in the defendant"s car a covert listening device which recorded words spoken by the defendant when inside the car. The device recorded the defendant"s end of telephone conversations on his mobile telephone but did not pick up any speech from the person on the other end of the telephone.

5.13 Since placing the listening device in the defendant"s car involved entry into private property, the entry would only be lawful if it was properly authorised under sections 91(5), 92 and 97(1) of the Police Act 1997.[5] The installation of a covert listening device inside a private car also constituted intrusive covert surveillance as defined under section 26(3), (4) and (5) of RIPA.[6] The police had obtained permission under both the Police Act 1997 and RIPA to conduct the investigation. The defendant was subsequently charged with offences of conspiracy to supply controlled drugs.

5.14 At a preparatory hearing of the case, the defence submitted that what had occurred was "interception" of the telephone calls, as defined by section 2(2) of RIPA, and that all the evidence of the product of the listening device was therefore inadmissible by virtue of section 17 of that Act. The trial judge ruled admissible evidence of recordings made by the listening device. The defendant appealed.

5.15 The appeal was dismissed. It was held by the English Court of Appeal that "interception" as defined under section 2(2) of RIPA denoted some interference or abstraction of the signal, whether it was passing along wires or by wireless telegraphy, during the process of transmission by a telecommunications system. Such a system involved the use of electrical or electromagnetic energy.

---

3 See Annex (B) of paper on admissibility of intercepted materials prepared by the Law Reform Secretariat.

4 [2004] 1 WLR 3279 (CA).

5 This meant that it needed first to be authorised by the Chief Constable of the relevant force and subsequently approved by a commissioner appointed for the purposes of the Police Act 1997 who will be a person either holding or having held high judicial office: see para 9 of the judgment in *R v E*.

6 See para 10 of the judgment in *R v E*.

5,16 The Court of Appeal further held that although what the defendant said into his mobile telephone was recorded by the covert listening device, the recordings were not made in the course of the transmission of the telecommunications. The recording process took place independently of the operation of the telecommunications system. What was recorded was not the transmission but the words of the defendant taken from the sound waves in the car. The court ruled that the recordings made through the use of the covert listening device placed inside the defendant‟s car were admissible as evidence.

5.17 The following passages in the Court of Appeal‟s judgment, delivered by Hughes J, set out the reasons for its ruling:

> *We are accordingly satisfied that, if what happened here was interception, evidence of the content of any telephone calls is rendered inadmissible by section 17(1)(a). If it was interception, it is therefore unnecessary to get as far as the discretionary power to exclude evidence pursuant to section 78 of the Police and Criminal Evidence Act 1984….It appears that the critical question is whether what occurred here was interception.*
>
> *We are not here concerned with recording both sides of the telephone conversations by one or other of the participants—something which sometimes is referred to as „participant monitoring‟. What happened here was that the listening device picked up what the defendant said in the car. It did not distinguish between what he said to a companion in the car and what he said into his mobile telephone. What he said into his mobile telephone was certainly recorded. The question is whether it was also, at those times when he was on the telephone, intercepted.*
>
> ...
>
> *In our view, the natural meaning of the expression „interception‟ denotes some interference or abstraction of the signal, whether it is passing along wires or by wireless telegraphy, during the process of transmission. The recording of a person‟s voice, independently of the fact that at the same time he is using a telephone, does not become interception simply because what he says goes not only into the recorder, but, by separate process, is transmitted by a telecommunications system. That view is consistent with the expressions contained in the Act to which we have drawn attention.*
>
> *Interception, moreover, as section 2(2) closely defines it, is concerned with what happens in the course of transmission by „a telecommunications system‟. Section 2(1) defines a „telecommunications system in the following terms: „Any system …which exists…for the purpose of facilitating „the*

transmission of communications by any means, involving the use of electrical or electromagnetic energy.' Thus, the system begins at point A with the conversion of sound waves from the maker of the call into electrical or electromagnetic energy.

What was recorded here was what happened independently of the operation of the telecommunications system. Of course, the recordings were made, questions of milliseconds apart, at the same time as the defendant's words were being transmitted. They were not, however, recordings made in the course of transmission. What was being recorded was not the transmission but the words of the defendant taken from the sound waves in the car." [7]

The Court of Appeal accordingly held that there was no interception for the purposes of RIPA.

The implications of the ruling in R v E

5.18 In *R v E*, the English Court of Appeal gave a clear explanation as to the distinction between the nature of the materials obtained through interception of telecommunications and those collected by means of covert surveillance, such as through the use of a covert listening device. The court relied on section 17 of RIPA to rule that materials intercepted during the course of transmission of telecommunications were not admissible as evidence, whereas materials obtained by other means of covert surveillance could be adduced as evidence in legal proceedings.

5.19 The principles elicited in the judgment are relevant to the question of whether there is reasonable justification for treating the admissibility (and hence the retention and destruction) of materials obtained through interception of communications differently from those obtained through covert surveillance.

~~It~~ is the fact that in the United Kingdom it has for many years been the approach of successive governments to telephone surveillance by way of interception, properly so called, that the content of interceptions may inform police investigations but may not form part of the evidence at any subsequent trial. That is the origin of section 17 of RIPA and its somewhat differently expressed predecessor, section 9 of the Interception of Communications Act 1985.

The reasons why this has been the approach in this country need not detain us in this judgment. They are referred to in the speech of Lord Mustill in R v Preston [1994] 2 AC 130, 146-148, 163-167. We need only record that the reasons for that

[7] Cited above, at 3283.

approach do not lie in any irrelevance or in any unfairness to an accused of evidence emanating from an interception. They lie in wider considerations of public interest in the confidentiality of methods of investigation and of the sources of information. Plainly, it was a deliberate choice of Parliament to maintain this position when RIPA was enacted.

This exclusionary rule of evidence, however well established a United Kingdom rule it may be, goes, however, significantly further than is required by either article 8 of the European Convention … Neither of those requires more than regulation of interference with communications; they do not require the exclusionary rule which is applied to this country. The facts behind the decision of the House of Lords in R v P [2002] 1 AC 146 illustrate this. What was in question there was the admissibility in evidence in an English criminal trial of recordings made via telephone interceptions in a foreign country; the foreign country was a party to the European Convention and the Convention had been part of its law for many years. In that country, such intercepted material is by law admissible in evidence in a criminal trial. A national framework of rules controls and authorises when interception can take place. That national framework of rules has been found by the European Court of Human Rights to be Convention compliant: see speech of Lord Hobhouse of Woodborough in R v P [2002] 1 AC 146, 153-154…."[8]

5.20 As indicated in *R v E*, whether materials obtained from interception of communications should be admissible depends on the relative importance attached by the legislature to the protection of the secrecy of a particular method of investigation and to the sources of information. However, the court pointed out that an exclusionary rule of evidence such as section 17 of RIPA goes beyond what is required for the protection of privacy under the European Convention for the Protection of Human Rights.

Background information: Hong Kong

The consultation paper on Privacy: Regulating Surveillance and the Interception of Communications

5.21 As pointed out at paragraph 5.3 of this report, the consultation paper recommended that materials obtained through surveillance and interception of communications should be inadmissible as evidence, regardless of their relevance.[9] In doing so, the sub-committee was following the approach in the United Kingdom *Interception of Communications Act 1985*:

---

[8] Cited above, at 3289.

[9] Paras 6.61 - 6.70, consultation paper.

"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.

…

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."[10]

The report on Privacy: Regulating the Interception of Communications

5.22 In its final report on *Privacy: Regulating the Interception of Communications* published in December 1996, the Law Reform Commission made the following recommendations regarding admissibility:

(1) Lawful interception of telecommunications

"We recommend that material obtained through an interception of telecommunications carried out pursuant to a warrant shall be inadmissible as evidence regardless of its relevance. For the purposes of this recommendation, 'telecommunications' means communications by electromagnetic means. This prohibition should cover not only the fruits of interception but also the manner in which the interception was made.

We recommend that no evidence shall be adduced and no question shall be asked in cross-examination which tends to suggest that an offence in relation to an interception of telecommunications has been committed or that a warrant authorising an interception of telecommunications has been issued."[11]

(2) Lawful interception of postal mail

"Different considerations apply, however, to material obtained through an interception of postal mail ….

We recommend that material obtained through an interception of communications transmitted other than by electromagnetic means which was carried out pursuant to a warrant shall be admissible as evidence and may be

---

10 Paras 6.68 and 6.70, consultation paper.

11 Paras 7.44 - 7.45, report on *Privacy: Regulating the Interception of Communications*.

retained for so long as may reasonably be necessary for the purpose of any criminal proceedings."[12]

(3) Unlawful interception of telecommunications

"We recommend that material obtained through an unlawful interception of telecommunications shall be inadmissible as evidence regardless of its relevance. The prohibition should cover not only the fruits of interception but also the manner in which the interception was made."[13]

(4) Unlawful interception of communications transmitted other than by electromagnetic means

"We recommend that material obtained through an unlawful interception of communications transmitted other than by electromagnetic means shall be admissible as evidence."[14]

(5) Exception for prosecution of the offence prohibiting interception of communications

"We agree that there should be an exception to allow evidence of interceptions to be adduced in court to prosecute an individual who is alleged to have committed the interception offence.

We recommend that material obtained through an interception of communications whether carried out with or without lawful authority shall be admissible in evidence in relation to proceedings for the offence prohibiting interception of communications."[15]

The Hong Kong Government's White Bill on Interception of Communications

5.23 In February 1997, the then Security Branch issued a consultation paper on its proposed *Interception of Communications Bill*. It adopted the recommendation made by the Commission that intercepted materials should not be admissible as evidence in legal proceedings. The

---

12 The Commission recommended, at paragraphs 7.46 - 7.49 of the report, that "*material obtained through an interception of communications transmitted other than by electromagnetic means which was carried out pursuant to a warrant shall be admissible as evidence and may be retained for so long as may necessary for the purpose of any criminal proceedings.*" This would include materials obtained through an interception of postal mail such as a letter or that part of a communication which consists of a physical document.

13 Para 7.61 of the report.

14 Para 7.63 of the report.

15 Paras 7.64 - 7.65 of the report.

proposal was stated as follows:

> *"~~–~~intercepted materials should not be admissible as evidence in the court to avoid revealing our law enforcement capabilities. Exception should be made where the intercepted materials are used to prove an illegal interception. In line with existing practice, intercepted materials which are physical items and which can be used to prove a criminal offence, for example, a postal article should also be admissible as evidence."*[16]

5.24 This approach was reflected in clause 11 of the White Bill, which reads:

> *"~~–~~11(1) Intercepted material and information obtained by interception under section 6 or 7 or unlawful interception…shall not be admissible in evidence in any proceedings before a court or tribunal other than to prove that an offence under section 3(1) or 4(1)(a) or (2)(a)(i), or section 24(c) or (d) of the Telecommunications Ordinance (Cap. 106), has been committed.*
>
> *(2) Any intercepted material and any particulars as to an interception…shall not be made available to any party to any proceedings, including the prosecution in any criminal proceedings.*
>
> *(3) In any proceedings before any court or tribunal-*
>
> *(a) evidence which tends to suggest that a warrant has been or is to be issued to an authorized public officer…shall not be adduced; and*
>
> *(b) a question which tends to suggest that a warrant…has been issued shall not be asked.*
>
> *(4) This section shall not be construed to preclude the admissibility in evidence of any intercepted material which is-*
>
> *(a) an item the possession, custody or control of which is an offence; or*
>
> *(b) a postal article seized under a warrant issued on an application under section 6(5)."*

[16] At para 10(g) of the consultation paper on *Interception of Communications Bill*.

The Private Members' Bill on Interception of Communications

5.25 On 23 April 1997, Mr James To introduced the Interception of Communications Bill as a Private Members' Bill into the Legislative Council. The Bill allowed the use of intercepted materials as evidence in court.

5.26 The Secretary for Security strongly opposed the Bill and argued that the Bill had been drawn up without prior consultation with the law enforcement agencies and "*would pose serious operational difficulties*" to the law enforcement agencies. It was further suggested that "[*s*]*ome of the proposals in the Bill will increase privacy risks and they run against the recommendations of the Law Reform Commission in its report on privacy*".[17]

5.27 The disadvantage envisaged by the Administration of allowing intercepted material to be used as court evidence was that that:

> *"It will entail public dissemination of personal information and was recommended against by the Law Reform Commission. It will, of course, also have the undesirable effect of revealing our law enforcement capabilities to intended criminals."* [18]

5.28 Mr James To responded that the Administration's arguments against the proposed admissibility of intercepted materials as evidence under the Bill were basically unacceptable:

> *"The Administration argues that, under certain circumstances, if law enforcing officers really have to produce materials to be used as court evidence, it may reveal the so-called law enforcement capabilities.*
>
> *I think there will always be such a contradiction. For instance, if an 'undercover agent' is deployed to collect information on a long term basis, his identity should not be revealed in courts for testification. Why? It is because if it is the case, the identity of the undercover agent will be known to all and the line through which crucial information is collected will be broken. The common saying for that situation is that the line 'has turned yellow' and that means the line is broken. The evidence can only be used for prosecution on that charge. You may say that it is not the case. The undercover agent might not have to appear in court and other evidence might be resorted to. Thus, the undercover agent would not have to show himself and could continue his undercover assignment. But from the point of prosecution, the problem is that it is not known whether it is sufficient to initiate a charge without the evidence of the undercover agent. Therefore, the argument is basically unacceptable because, even though other methods are available, you still have to decide whether to reveal the method*

---

17 Record of meetings of the Legislative Council dated 27 June 1997, at 1502-1505.

18 Cited above, at 1504.

or continue to collect evidence by that method. Also, much of the so-called advanced technology can in fact be used more than once."[19]

The Interception of Communications Ordinance (Cap 532)

5.29 The Private Members' Bill on Interception of Communications was subsequently enacted on 28 June 1997 as the Interception of Communications Ordinance (Cap 532). However, the Ordinance has not yet come into force.

5.30 The admissibility of evidence obtained through interception of communications is provided for under section 9 of the Interception of Communications Ordinance, the relevant parts of which read:

> *"(2) In any proceedings, if it is represented to the court that the intercepted material relied on by the prosecution as evidence against the accused was or may have been obtained in violation of section 3, the court shall not allow the material to be given as evidence against the accused unless the prosecution proves beyond reasonable doubt that the material was not obtained as aforesaid.*
>
> *(3) The court can of its own motion require the prosecution to prove that the intercepted material was not obtained in violation of section 3.*
>
> *…*
>
> *(8) In any proceedings, the court may refuse to admit intercepted material as evidence against the accused if it appears to the court that having regarded to all the circumstances, including the grounds upon which the interception was authorized and the application procedure for the authorization, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it."*

5.31 The approach followed by the Interception of Communications Ordinance was that materials obtained by lawful interception should be admissible in evidence subject to relevance and to judicial discretion (which has been given statutory backing under section 9(8) of the Ordinance) to exclude admissible evidence to ensure the fairness of the proceedings.

5.32 By virtue of section 9(2) of the Ordinance, materials obtained by an interception which has not been conducted in accordance with the requirements of the Ordinance would not be admissible as evidence.

---

[19] Cited above, at 1509.

Background information: United Kingdom

The Interception of Communications Act 1985

5.33 Section 9(1) and (2) of the United Kingdom Interception of Communications Act provided:

> *"(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest -*
>
> *(a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below; or*
>
> *(b) that a warrant has been or is to be issued to any of those persons.*
>
> *(2) The persons referred to in subsection (1) above are-*
>
> *(a) any person holding office under the Crown;*
>
> *(b) the Post Office and any person engaged in the business of the Post Office; and*
>
> *(c) any public telecommunications operator and any person engaged in the running of a public telecommunication system."*

5.34 An explanation of the rationale for the exclusion of intercepted materials under the 1985 Act was given by Lord Hobhouse in *R v P*[20]:

> *"Any developed society has to have a scheme for the surveillance of those who are liable to attack or prey upon the society of members. Such scheme has throughout history included the interception of communications and in modern times this has included telecommunications. This in turn has led on to the need for laws to limit and control such interceptions particularly where publicly provided or sponsored means of communications are involved. …This then leads on to the question: on what basis is the government to be permitted to carry out the surveillance necessary for the health and survival of the society in which we live? Section 2 of the Act accordingly provided for the Secretary of State to issue warrants authorising*

[20] [2002]1 AC 146.

and requiring interceptions of communications by post or public telecommunication systems to be carried out. …

But then a further question arises. If the interception results, as no doubt will not infrequently be the case, in the obtaining of evidence which will assist in the conviction of criminals, are the authorities going to use that evidence in court to assist in the prosecution of the criminals concerned? Other things being equal all relevant and probative evidence is admissible. But where surveillance evidence is concerned the use of the evidence comes at a price. If the fairness of the trial is to be preserved the defendant must be permitted to probe the evidence and question the witnesses who come to court to provide the proof. This means that disclosure has to be made and the secrecy of the means and extent of the surveillance has to be sacrificed. This is a real problem for those involved in the prevention and detection of crime as the cases involving informers and concealed cameras have shown. The solution traditionally adopted by the authorities has been to elect for the maintenance of secrecy and to prefer this to the use of covertly obtained material in court. This was the choice made in the 1985 Act. Section 9 of the Act prevents any questions being asked in court which tend to suggest that an official may or may not have had authority under the Act to intercept a communication. In making this choice the Government were following the same approach, making secrecy the paramount consideration, as they had urged upon the Birkett Committee in 1957 (Cmnd 283) and was accepted by that committee. Other provisions of the Act, most notably section 6 limiting the dissemination and requiring the destruction of intercept material, are also designed to preserve secrecy.

The oblique wording of section 9 is clearly directed to preserving the secrecy of any surveillance operation covered by the Act. …"[21]

5.35 The purpose of section 9 of the Act (which prevented any questions being asked in court which tended to suggest that a warrant for interception of communications had been, or was to be, issued to any official) was to preserve the secrecy of surveillance operations, at the cost of excluding the use of covertly obtained materials in court.

5.36 However, where the 1985 Act did not apply, surveillance evidence was in principle admissible, subject to section 78 and the ordinary safeguards. As held by the House of Lords in *R v P*:

"… In this country it is, in the judgment of the Government, the necessity to have a fully effective interception system which

[21] Cited above, at 162.

creates the necessity for secrecy and consequently the need to keep the evidence of it out of the public domain. But where secrecy is not required, the necessity is that all relevant and probative evidence be available to assist in the apprehension and conviction of criminals and to ensure that their trial is fair. …"[22]

5.37 The general principle on admissibility of evidence obtained by unlawful means was reiterated by the House of Lords in *R v P*:

—It should be noted that the court again emphasised that the defendant is not entitled to have the unlawfully obtained evidence excluded simply because it has been so obtained. What he is entitled to is an opportunity to challenge its use and admission in evidence and a judicial assessment of the effect of its admission upon the fairness of the trial as is provided for by section 78."[23]

Consultation Paper by the Secretary of State for the Home Department on "Interception of Communications in the United Kingdom"

5.38 In June 1999, the Secretary of State for the Home Department presented a consultation paper entitled *Interception of Communications in the United Kingdom* to the United Kingdom Parliament. The paper considered the arguments for and against lifting the ban on the use of telecommunication intercepts in evidence and invited suggestions for a regime which would enable intercept material to be used in evidence and to make appropriate disclosures to the defence, bearing in mind the effects upon sensitive information, resources and the efficient operation of the criminal justice system:

—8.1 Section 9 of the Interception of Communications Act 1985 has the effect of prohibiting the evidential use of intercept material gathered under a warrant issued under the Act. The value of this provision has been the subject of much debate over the years, with opinions sharply divided. More recently, the use of foreign intercept material in UK trials has highlighted the difference between our practice and that of Europe.

8.2 There are strong arguments both for the repeal and retention of this particular part of IOCA. Those seeking repeal believe use of this material is one of the few ways of gathering evidence against those who plan crimes but engage others to carry them out. The Inquiry into Legislation Against Terrorism, undertaken by Lord Lloyd addressed the law on interception evidence,

[22] Cited above, at 165.
[23] Cited above, at 161.

recommending that section 9 of IOCA be amended so as to allow the prosecution to adduce intercept material in cases affecting national security….'.

8.3 The main counter-argument, for retention of the prohibition on evidential use, is that exposure of interception capabilities will educate criminals and terrorists who will then use greater counter interception measures than they presently do. This would mean that any advantage gained by repeal would be short lived and would make interception operations more difficult in the longer term.

8.4 In addressing this part of IOCA, the Government will have to bear in mind the requirement of Article 6 of the European Convention on Human Rights, which guarantees the right to a fair trial. Implicit in this guarantee is the principles that there must be 'equality of arms' between the prosecution and the defence in criminal proceedings. Any rule of evidence or procedure which favours one party over the other may conflict with this principle.

8.5 The question of whether section 9 of IOCA undermines the principle of 'equality of arms' and introduces an unfairness into proceedings where interception played a part in the investigation was addressed by the European Commission in the case of Preston v UK. The applicants claimed, amongst other things, that their trial was unfair because knowledge of material gathered through interception of communications gave the prosecution an advantage in preparing their case. They also claimed that the use in evidence of data relating to communications, while interception material was excluded, amounted to an inequality of arms. The Commission did not agree, noting that section 9 prevented either party adducing evidence which could tend to suggest that interception had taken place. The Commission did not consider that the applications had shown how access to interception material by the police had any effect on subsequent proceedings, or in what respect that material was used to the applicants' detriment in preparing the prosecution case, other than to provide the prosecuting authorities with a starting point from which to gather admissible evidence against the applicants. The Commission, by a majority, declared the application inadmissible.

8.6 In many other European states, intercept evidence is used in criminal cases and, so far as Article 6 is

concerned, this practice has been approved by the European Court. See for example, Valenzuela Contreras v Spain (30 July 1998) and Lambert v France (24 August 1998).

8.7 However, in those States interception is generally ordered by an investigating judge. The United Kingdom is in a different position, since criminal investigations are not supervised by judges but by the law enforcement agency. For that reason, the principle of equality of arms as between prosecution and defence will be particularly relevant in devising any system which allows the use of intercept material in evidence. Furthermore, any arrangements which make intercept material available to one or both parties would have to be both practical and affordable.

8.8 To date, no satisfactory arrangements have been found. Nevertheless, the Government continues to work on the question, and would welcome the views of others.

The Government welcomes suggestions for a regime which would enable intercept material to be used in evidence and to make appropriate disclosures to the defence, bearing in mind the effects upon sensitive information, resource and the efficient operation of the criminal justice system."

The Regulation of Investigatory Powers Act 2000 (RIPA)

5.39 The United Kingdom Government's intention was to bring all forms of interception within Part 1 of RIPA so that the 1985 Act would be superseded and could be repealed.[24] It was clear from the new provisions that the Government did not accept the case for removing the ban on the use of intercepted telecommunications.

5.40 Section 17 of part I of RIPA is based on section 9 of the 1985 Act, but expresses the prohibition on the use of intercept materials in less oblique terms. Section 17 provides:

—subject to s.18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) -

(a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any

[24] Part 1 of RIPA has repealed the key sections of the 1985 Act, including sections 1 to 10 and section 11(2) to (5) of the 1985 Act.

of the contents of an intercepted communication or any related communications data; or

(b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur."

5.41 Section 17(2) covers:

"(a) conduct … that was or would be an offence under s 1(1) or (2) of this Act or under s 1 of the … 1985 Act;

(b) a breach by the Secretary of State of his duty under section 1(4) of this Act;

(c) the issue of an interception warrant or of a warrant under the …1985 Act;

(d) the making of an application by any person for an interception warrant, or for a warrant under that Act;

(e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant."

The House of Lords debates on the Regulation of Investigatory Powers Bill 2000

(a) The case for repeal of the prohibition on use of intercept product as evidence

5.42 The question of whether clause 16 (which has now been enacted as section 17 of RIPA) dealing with exclusion of matters from legal proceedings should stand as part of the Bill was raised in the House of Lords debate on 19 June 2000. Lord Lloyd opposed the retention of the clause excluding intercept material from being used as evidence in court. He stated the arguments as follows:

—…The only point of detail I wish to make is on Clause 16. As my views on Clause 16 are very well known to the Home Office — I explained them at great length in chapter 7 of my report on terrorism - nothing that I shall say will take the Minister by surprise.

Clause 16 replaces the old and – I think I can call it — notorious Section 9 of the Interception of Communications Act 1985. It was notorious because the drafting was so oblique that it took three, perhaps even four, decisions of the House of Lords before the meaning was made clear. Clause 16, which replaces

Section 9, is in comparison relatively clear, although it needs to be read several times before its meaning springs to the eye. The purpose is exactly the same in both cases; namely, to prohibit the disclosure of the contents of an interception in proceedings in a court of law. That means that the intercept can be used to catch the criminal, but the intercept cannot be used to convict the criminal.

I confess I have never understood the logic of that — and I have been involved in matters concerning the interceptions of communications for … 15 or more years. … Perhaps I may take a case where the police or the Security Service are hot on the trail of a terrorist gang or international conspiracy for the importation of a hard drug such as heroin. The authorities will apply for a warrant ….Having secured their warrant, let us say that the interception proves successful. The officer overhears a conversation in which a propose importation of drugs is discussed and those who are to take part in it are named. If we suppose that the importation cannot be prevented, in due course it takes place but, happily, the importers are arrested. They are then put up for trial.

Obviously, the tape recording used in the interception would be highly relevant and cogent evidence to convict those who had been arrested. In law, all relevant evidence is prima facie admissible evidence. Given that, why should the tape recording of such a telephone conversation, which would secure the conviction of the drug importers, not be used in court? It simply does not make sense.

… perhaps I may make two brief points. The first is that evidence of telephone communications of that kind is admissible in court in every country in the world as far as I am aware. The countries I visited during my inquiry into terrorism — France, Germany, the United States and Canada — regard such evidence as indispensable. They were astonished to hear that we do not use it in this country.

Secondly, let us suppose that, instead of applying for a telephone intercept under Part I of the Bill, the police decide to go for an authorisation under Part II to enable them to place some intrusive device, a bug, in some convenient sport, perhaps even in the very telephone from which the telephone conversation is made. Let us suppose that, as a result, there is a tape-recording of the same conversation as might have been recorded by the telephone intercept. The tape-recording obtained by means of a bug is admissible in evidence. At once that poses the question: why should the tape-recording be admissible when it is obtained by means of a bug and not

admissible when it has been obtained by a telephone intercept? It simply does not make sense.

That that is intended to be the position is clear from the fact that in Part II of the Bill there is nothing that corresponds to Clause 16 in Part 1. Again, I ask the question, why should the evidence be admissible in the one case but not in the other? It cannot have anything to do with the Human Rights Act — in case that is the suggestion. There is no difference from a human rights point of view whether the bug is placed in the terrorist's room or whether the terrorist has his telephone conversation intercepted. Indeed, if I were a terrorist, I should be more concerned at the thought of the police or the Security Service intruding in my home than I should be if they listened to my telephone conversations. I hope that, in due course, the Minister will be able to explain why there is this difference between Part I and Part II of the Bill.

…

The position now is that if a telephone conversation takes place in England, evidence of that telephone conversation will be admissible in court if the interception takes place in Holland but not if the interception takes place in England. I suggest that that is not absurd but unjust. Justice is as much concerned with the conviction of criminals as with the protection of human rights.

I now come to the reasons that the Minister will give. He will say that the police and Customs services have always been opposed to the repeal of Section 9. I shall be very surprised if the noble Lord says that the Security Service is opposed to the repeal, because I know for a fact that it is not. The reason given by the police for wanting to continue with Section 9 is their fear that if criminals realise for the first time that their conversations may be tape-recorded, they will cease to use the telephone for hatching their plans. I regard that objection as utterly unrealistic.

Terrorists and international drug dealers are not simple souls who have never heard of telephone tapping; they are hardened, sophisticated, professional criminals who know every bit as much about telephone tapping as anybody in this Committee — probably a great deal more. I suggest that the notion that they will give up using the telephone to hatch their schemes because evidence of what they say in a telephone conversation will be admitted in court of law is fanciful. They must communicate with each other in some way. As I said in my report, they cannot communicate by pigeon post and have no alternative but to use the telephone. They will continue to use the telephone. If the police believe otherwise, they are, with all respect, wrong.

We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so.

I know that there are other difficulties to which the Minister may refer. There is said to be a difficulty in relation to the disclosure of what is called unused material. But with good will and a measure of ingenuity I do not doubt that those difficulties could be overcome.

I do not expect the Government at this stage to agree with a point that I have been putting forward fairly consistently, I hope, for many years. I oppose the Question that this clause stand part of the Bill because people should know that so long as Clause 16 remains on the statute book we shall be fighting organised crime with one arm tied behind our backs. It is the terrorists and the international drug dealers who will have the loudest laugh."[25]

(b) The Government's case for retention of the prohibition on use of intercept product as evidence

5.43 Lord Bach accepted that the arguments from Lord Lloyd were powerful and persuasive. However, he put forward the Government's position as follows:

—…The basic question is this. Should an intercept product be admissible as evidence in court? ... this type of evidence is not admissible at present because of the Interception of Communications Act 1985 … .the question has been addressed many times in recent years …. the Home Secretary held a seminar last year at which the future of this existing section of the Interception of Communications Act was the sole item on the agenda. A range of views was expressed and I am told that the balance came down in favour of retaining the existing provision…

Subject to certain exceptions set out in clause 17 [which is now section 18 of the RIPA], this clause excludes evidence, questioning or an assertion in legal proceedings likely to reveal the existence or absence of a warrant. Clauses 16 and 17 [now sections 17 and 18] cover more ground than does the original

[25] House of Lords Hansard for 19 June 2000, cols 107 -110.

position and are in response to some of the questions that have arisen over the years as to the applicability of Section 9 in certain cases.

… Why not use the product of interception warrants evidentially? First, the current prohibition on the use of evidence has worked well since the Act came into force. The existing regime has stood the test of time and offers valuable protection to privacy, which an evidential regime would not.

Secondly - perhaps this is the main argument - in a fast-moving communications industry, it is vital that the existing capacity is protected. Exposure of interception capabilities would or might educate criminals and terrorists who might then use greater counter-interception measures than they presently do. We believe that it is vital that the existing capability is protected and that the exposure of interception capabilities, which would result, as night follows day, from a repeal of the prohibition, would educate criminals and terrorists. They would certainly use greater counter-interception measures than they presently do and the value of interception as an investigative tool - it is a valuable investigative tool, particularly against the most serious criminals and terrorists - would be seriously damaged.

For those reasons, we are not convinced that a change to an evidential regime would involve a rise in criminal convictions in any more than the short term. Criminals and terrorists would become ‗wise' to it. The Government have considered the subject many times and have carried out a number of specific studies, including most recently research into the experience of seven other countries in operating an evidential regime. We are the first to admit that the issue is finely balanced. The decision to retain a version of Section 9 is supported by the majority of respondents - which is hardly a convincing argument in itself - to the consultation paper. It has helped us decide that we are right in believing that the prohibition should be maintained. …

The arguments for the repeal were made most persuasively tonight by the noble and learned Lord. I shall try to deal with one or two of the issues that he raised. So far as concerns the argument for educating criminals, of course everyone knows that telephones can be intercepted, but they do not always know the exact capability, how quickly interception warrants can be sought, which networks are capable of interception and so on. We attempt to keep a step ahead by not revealing that capability.

The noble and learned Lord drew the contrast between evidence from a bug and that from a phone tap. It is arguable that different considerations exist. Phone taps rely on third parties - Post Office staff, for example - and use more sophisticated

techniques. Bugs are employed and placed by law enforcement security agencies, and their capacity is relatively well known, unlike some of the details of interception capability. However, it would be an abuse of Part II powers, referred to by the noble and learned Lord, to plant a bug on a telephone simply in order to avoid the non-evidential rule in Part I. That is already made clear in the code of practice under the Police Act 1997.

I repeat that this issue is finely balanced and of considerable importance. The case could not be put better than it was by the noble and learned Lord. For our part, we are persuaded that our course is the better one. In spite of the disadvantages which clearly lie in not allowing interception evidence to be given, we believe that strong arguments exist on the other side.

I turn to the matter of other European countries. The noble and learned Lord made the point that other countries allow intercept evidence. In fact, he believes that that is the case in every other country, and I am certainly not in a position to argue with him. We do not believe that a direct comparison is possible. In countries which allow intercept material to be used, the interception warrant is generally ordered by the investigating judge. In this country, obviously criminal investigations are not supervised by judges but by law enforcement agencies. We are concerned that it would be difficult, if not impossible, to devise a system that would ensure equality of arms between prosecution and defence which is both practicable and affordable. We believe that the present system does that; in other words, neither the prosecution in the vast majority of cases nor the defence knows of the existence of the interception that may have taken place.

I have attempted to explain fairly briefly why we believe that the course that no doubt successive governments have taken on this particular issue is the right one with which to continue. However, it would be ridiculous for me to say that this is not still a live issue and to which we shall return at various times."[26]

5.44 Clause 16 of the Regulation of Investigatory Powers Bill was duly enacted as section 17 of RIPA.

Report by the Newton Committee in December 2003 on review of terrorism legislation

5.45 On 18 December 2003, the Newton Committee (headed by Privy Councillor Lord Newton), set up by the Secretary of State for the Home Department to review the *Anti-terrorism, Crime and Security Act 2001* enacted

[26] Cited above, cols 111-112.

following the attacks on 11 September 2001, published its report. The report recommended that the blanket ban on the use of intercepted communications in court should be relaxed:

> —208 *In our view, one way of making it possible to prosecute in more cases would be to remove the UK's self-imposed blanket ban on the use of intercepted communications in court. This was also the view reached by Lord Lloyd in his 1996 Report, to which we have seen no convincing response, and by Lord Carlile when giving evidence to the Home Affairs Select Committee on his review of the operation of Part 4.*
>
> 209. *The Government did not accept the case for removing the ban on the use of intercepted communications as evidence when the Regulation of Investigatory Powers Act 2000 replaced the Interception of Communications Act 1985. The reasons given were, essentially, that allowing the use of intercepted communications as evidence would reveal the authorities' capabilities, prompting criminals to take more effective evasive action. More recently the Home Secretary has said that the issue is under review, and we understand that the review is likely to continue into the New Year.*
>
> 210. *The Regulation of Investigatory Powers Act 2000 forbids the use of domestic intercepts in UK court proceedings. There is, however, no such bar on the use of foreign intercepts obtained in accordance with foreign laws. Nor is there a bar on the admission of bugged (as opposed to intercepted) communications or the products of surveillance or eavesdropping, even if they were not authorised and were an interference with privacy. There is no bar on foreign courts using British intercept evidence if the intelligence and security services are prepared to provide it.*
>
> 211. *Other than the Republic of Ireland we have not been able to identify any comparable country with such an extensive ban. In international operations (such as against al Qaeda) the USA has published details of its intercept capacity of landlines, mobile phones, satellite phones, diplomatic correspondence, and satellite intercept of communications.*
>
> 212. *We understand the concerns of the intelligence and security services, which include not only the protection of sources and methods but also the need to ensure that interception for intelligence purposes is not impeded by the imposition of complex procedures to meet evidential*

requirements. We recognise that a balance has to be struck between the public interest in prosecuting particular cases and the public interest in maintaining the effectiveness of intelligence gathering techniques and capabilities. We consider, however, that the balance has not been struck in the right place if intercepted communications can never be used evidentially.

213. Relaxing the ban would not place an obligation on the prosecution to use intercepted evidence. We can also see the case for modifying the normal rules governing the disclosure of evidence so that, for example, the prosecution would not be obliged to disclose intercept evidence, or even its existence, unless they chose to rely on it. This would need to be done with care to minimise the risk of miscarriages of justice, but those risks should not be greater than under the present system where the prosecution is forbidden from disclosing intercepted communications, even if they are exculpatory.

214. Consideration could also be given to have different classes of warrants authorising the interception of communications, some allowing evidential use of the product and others not. This is the approach taken by some other countries (where interception by the police and investigating judges can be used evidentially).

215. It is important that making intelligence available for prosecution does not compromise the collection and use of intercepted communications for intelligence purposes. We hope that the current review can devise a system which meets both needs."

5.46 The Newton Committee also made recommendations on the disclosure of material to alleviate the law enforcement agencies‟ concern at the obligation to disclose all intercept product as unused materials to the defence:

—22. It is an important principle under the British system of justice that all the available evidence must be produced in the presence of the accused at a public hearing with a view to adversarial argument. The defence normally has the right to see all potentially relevant material, even if the prosecution is not relying on it (because it may undermine the prosecution‘s case). The parties argue out the significance of the evidence in court, where the judge‘s role is effectively that of an umpire, and the jury decides whether the prosecution‘s case is made.

229. Making all potentially relevant material public might serve the interests of a fair adversarial trial, but it could undermine the public interest if it revealed intelligence sources or techniques and so impaired the ability to gather intelligence. Nevertheless, there is an obvious public interest in prosecuting terrorists. The challenge is to achieve this fairly without compromising intelligence.

230. The disclosure rules are complex, and there are exceptions. For example, the doctrine of public interest immunity (PII) enables the prosecution to withhold material where the trial judge is prepared to agree that the public interest in non-disclosure outweighs the defendant's interest in having full access to all the relevant material. In doing so, the judge is required to carry out a 'balancing exercise', weighing the likely effects of disclosure against the need to ensure justice (which encompasses the potential relevance of the material to the defence). PII does not seem to be a complete answer to Part 4 cases because, by definition, sensitive information is so central to them. The judge would be obliged to apply the doctrine that the public interest in the fair administration of justice always outweighs that of preserving the secrecy of sensitive information where its non-disclosure may lead to an injustice and in many cases the judge might order potentially exculpatory material to be disclosed. The prosecution's only alternative to disclosure would then be to drop the charge."

5.47 The Newton Committee also put forward proposals for more structured disclosure rules for the specialised purpose of handling terrorism cases, where conventional prosecution might risk disclosing sensitive sources, or the available intelligence might not be admissible as evidence.

—26. It is possible that, in some cases, the prosecution could be inhibited by the risk that it will be required to disclose sensitive information in the discovery process, even if it is not relying on it, because it could help the defence.

237. The USA has a procedural statute called the Classified Information Procedures Act (CIPA). It does not change either the substantive rights of the defendant or the discovery obligations of the government. It is designed to balance the rights of a defendant with the interest of the state to know in advance the extent of the potential threat to its national security from pursuing a criminal prosecution. Each of CIPA's provisions is designed to prevent unnecessary or inadvertent disclosures of

classified information and to ensure that the Government is in a position to assess the national security 'cost' of proceeding with its case.

238. For example, to the extent that the court rules that certain classified material is discoverable, the prosecutor may seek the court's approval to use alternative measures such as deletion of sensitive information, substitution of summaries, closing the court, allowing witnesses to remain anonymous, requiring the defence to make its case known earlier in the process, and only allowing the defendant's security-cleared counsel to have access to the sensitive material.

239. Although the present public interest immunity rules in the UK already permit a certain amount of editing and summarisation there would, in our view, be merit in developing a more structured disclosure process that is better designed to allow the reconciliation of the needs of national security with the rights of the accused to a fair trial."

The proposed amendment to the Serious Organised Crime and Police Bill 2005

5.48 In February 2005, the Conservative Party proposed an amendment to the *Serious Organised Crime and Police Bill* to permit intercept material to be admissible in evidence. The Government opposed the amendment, which was defeated by a majority of 124 to 113.

5.49 The amendment to the Bill proposed that sections 17 and 18 of RIPA "*shall cease to have effect*." The case for the amendment was stated as follows:

—We argue that the present restriction is anachronistic and illogical, and its abolition has been recommended repeatedly to the Government in recent years. Our amendment does not alter the circumstances in which an interception warrant can be issued or renewed under the Regulation of Investigatory Powers Act 2000. Britain finds itself isolated, since with the exception of Ireland intercept evidence may be used to support criminal prosecutions in every other major country. The Government's argument that the use of intercept evidence could undermine the public interest by revealing to terrorists and organised criminals vital operational details deployed by the police and intelligence service, is I submit, complete nonsense, since a well established and refined system already operates in the criminal courts to ensure the withholding of operational details in circumstances in which disclosure would be detrimental to the public interest. …

At this early stage in the debate, it is important to point out that the new clause does not require the prosecution to use the intercept evidence during a criminal trial. Instead, the new clause is permissive, in the sense that it would afford the prosecution the opportunity to adduce intercept evidence in a case in which the prosecution lawyers believe that it is appropriate to do so. At present, apart from in a small number of eclectic and in some cases random exceptions, that course of action is not open to them. …

Shutting out telephone tapping evidence is contrary, as I understand it, to the basic principle of evidence - if it is relevant, it is admissible. …

Turning to how intercept evidence is used in other countries throughout the world, hon Members will appreciate that it is routinely deployed by prosecuting authorities in the United States and European countries with the exception … of ourselves and southern Ireland. …

As I said in Committee, Lord Lloyd of Berwick explained foreign countries' position on the use of intercept evidence in his inquiry into anti-terrorism legislation, which was published in 1996:

> *The first and most obvious argument is that evidence of intercepted material is admissible to prove guilt in each of the countries which I have visited, and in every other country of which I have knowledge. The United Kingdom stands alone in excluding such material. Thus in the United States the use of intercept material in evidence is regarded as essential. In many instances, including high-profile cases involving the New York Mafia, convictions otherwise unobtainable have been secured by the use of intercept material. I put to officers of the FBI the suggestion that they were having second thoughts about the use of intercept material. I could find no support for this suggestion. …*
>
> *In France I was told that intercept material has proved very valuable in terrorist cases. Thus, some 80 per cent, of the evidence against those suspected of involvement in the 1995 bombings is derived from intercept. Similarly, in Australia interception is regarded as an —extremely valuable aid to criminal prosecution" '… 664 prosecutions for offences ranging from murder to serious fraud were based on intercepted*

material, nearly 500 of those prosecutions being for drug offences. Convictions were obtained in 87 per cent of the cases. Often, when presented with the evidence of an intercept, the defendant pleads guilty.'

This is Lord Lloyd's considered opinion.

In Canada, the use of lawful interception evidence in court has been highly successful, with a conviction rate of more than 90 per cent. In 2001, lawful interception access helped to arrest approximately 100 organised criminals and solved 13 murder cases involving those individuals. In 2000, lawful interception process in the seizure of more than $100 million in drugs and the conviction of several criminals for importing or producing drugs.

In America, Congress passed the Omnibus Crime Control and Safe Streets Act in 1968. Title 3 of that Act contained the first comprehensive federal legislative framework governing electronic surveillance for use in criminal investigations. Between 1987 and 1997, electronic surveillance conducted pursuant to title 3 assisted in the conviction of more than 21,000 criminals….

In Britain, a chorus of heavyweight, authoritative and expert opinion — most recently, Metropolitan Police Commissioner Sir Ian Blair — favours lifting that ban. As I have said, Lord Lloyd recommended lifting the ban on the use of intercept evidence in his review of anti-terrorist legislation in 1996. The recommendation was made again in the debate on the Regulation of Investigatory Powers Act 2000, section 17 of which maintains the ban on the use of intercepted evidence in court that was previously contained in the Interception of Communications Act 1985.

…most recently the Newton committee, which was composed of senior Privy Councillors led by Lord Newton, published a report into the Anti-terrorism, Crime and Security Act 2001 on 18 December 2003. That report recommended that the blanket ban on the use of intercepted communications in court should be relaxed. …

The Government did not accept the case for removing the ban on the use of intercepted communications as evidence when the Regulation of Investigatory Powers Act 2000 replaced the Interception of Communications Act 1985. The reasons given were, essentially, that allowing the use of intercepted communications as evidence would reveal the authorities' capabilities, prompting criminals to take more effective

evasive action.

The Regulation of Investigatory Powers Act 2000 forbids the use of domestic intercepts in UK court proceedings but no such bar exists to the use of foreign intercepts obtained in accordance with foreign laws. Bugged, as opposed to intercepted, communications or the products of surveillance or eavesdropping are also not barred, even if they were not authorised and were an interference with privacy. There is no bar on foreign courts using British intercept of evidence, it the intelligence and security services are prepared to provide it. …

I want briefly to discuss the compatibility between the use of intercept evidence and the European Convention on human rights, which I mentioned earlier. Intercept evidence does not infringe the ECHR, whereas house arrest does. The ECHR is clear: intercepted communications do not infringe human rights and liberties provided that they are used proportionately. In other words, intercepted communications must serve a pressing need and be utilised in accordance with the law and in pursuit of one of the legitimate objectives spelled out in article 8(2). Article 8(2) refers to acting

> *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.'*

In respect of article 6, the Khan v United Kingdom case clarified the legitimacy of using intercept-type surveillance evidence. In respect of article 8, the case … verified the fact that the use of intercept communications complies with UK law and is compatible with the article. …

Why are the Government so set against the use of intercept evidence in court? That is the next question that we must consider. The Government's argument for non-disclosure of this evidence has been based on the following rationale: first and foremost, technology is changing so fast that any regime put in place would soon be outdated; secondly, the fear that allowing intercept evidence heard in court could compromise national security, damage relationships with foreign powers or the intelligence services, or threaten the lives of sources; thirdly, they are also of the opinion that there is a widespread misconception that the making of intercept evidence admissible would increase the chances of convicting detainees; fourthly, the final argument is that once intercept evidence has been disclosed there may be a requirement to

disclose the whole of the tapped conversation. That could be a passage of 10 minutes but one that had been tapped for a number of years.

These arguments have not persuaded many. Justice, the all-party law reform group, has also addressed the arguments advanced by the Government. It states:

> *'If the intelligence services of the United States, France, Israel, Canada and Australia can survive the use of such evidence in their courts, then British spies are surely equal to the challenge.'*

The Director of Public Prosecutions, Ken Macdonald, has made it clear that he backed the idea, and anti-terrorist sources stated that MI5 and MI6 have no objection in principle to such a move, but that the time and resources required to allow the product of telephone taps to be used as evidence in court would far outweigh the potential disadvantages.

What is the problem? The Government did not accept the case for removing the ban on the use of intercepted communications as evidence when the Regulation of Investigatory Powers Act 2000 was before the House, which replaced the Interception of Communications Act 1985. That was because they felt that allowing the use of intercepted communications as evidence would expose the authorities' capabilities, allowing criminals to take more effective evasive action. That, with the greatest respect, is complete nonsense. To begin with, it is not the impression that one gains from reading Lord Lloyd's recommendations on the matter. It also assumes that British serious criminals are a peculiarly insular lot whose information gathering does not penetrate far overseas.

In international operations, such as those against al-Qaeda, the US has published details of its intercept capacity in respect of landlines, mobile phones, satellite phones, diplomatic correspondence and satellite intercept of foreign communications. While the concerns of the intelligence and security services are understandable, it is clear that a balance needs to be struck between the public interest in prosecuting cases and the public interest in maintaining the effectiveness of intelligence-gathering procedures and capabilities. By excluding the use of potentially critical intercept evidence in the courts, this balance has not been struck. …

I remind the House that, under the new clause, relaxing the ban would not place an obligation on the prosecution to use intercept evidence. It would simply allow the submission of

intercept evidence in court and stand on a par with what is available to other agencies dealing with serious crime and terrorism. What is more, there are already eclectic and disparate cases in which intercept evidence is used in criminal courts, albeit as an exception to the general rule, and there has not been any damage to police or intelligence service operational capabilities and methodology. I submit that these experiences puncture the Government's objections to the use of intercept evidence and render the present state of the law in this area quite ludicrous. …

I turn briefly to the proper procedures and safeguards for non-disclosure that are already in place --…The House will know that, as a general rule, the prosecution has to disclose all material that it possesses — for and against its case. However, under the Criminal Procedure and Investigations Act 1996, applications can be made to the court when there is a dispute about whether the prosecution should disclose certain material in the public interest. When the prosecution prepares its list of materials to hand over to the defence, it can indicate which material it considers it need not disclose because of public interest immunity. It must also consider the relevance of the material. Where vast quantities of intercept are not relevant to any issue relating to the case, the disclosure rules do not require that this material be disclosed, irrespective of any question of public interest immunity.

To protect against any compromise in national security or to protect sources' lives, the prosecution's duty to disclose evidence is limited, so it need not disclose material where the public interests so dictates. In some cases, the prosecution will take the view that the material should be withheld — for example, where it is so sensitive that it is subject to public interest immunity. The prosecution must have genuine arguments for not disclosing material on public interest immunity grounds, which provide added protection for the defendant.

Public interest immunity also helps the UK to co-operate with other countries, because it allows the police and other prosecuting bodies to keep out of court sensitive material that other countries do not want published. So contrary to the Government's claim, the use of intercept material would not have a negative effect on the relationship between British and foreign security agencies. …

The withholding of sensitive information is an uncontroversial and unexceptional daily occurrence in the criminal courts. There is a clear public interest in preserving the anonymity of informers; of the identity of a person who has allowed his

premises to be used for surveillance, and of anything that would reveal his identity or the location of his premises; of other police observation techniques; and of police and intelligence service reports, manuals and methods. The police order manual, for example, is protected from disclosure. Techniques relating to intercept systems, procedures, technology and methodology fall into the same category. …

To summarise my case, almost every other country, including the US, allows the use of intercept evidence in court. Such evidence is deployed in those countries with significant success in cases involving organised crime and terrorism. Independent reports by Lords Lloyd and Newton, and 1999's consultation paper on the intercept of communications, recommended the use of intercept material as evidence. The use of such evidence is consistent with the principles of the European convention on human rights, and the law already permits its use."[27]

5.50 The Parliamentary Under-Secretary of State for the Home Department gave the following reply to the proposal to lift the ban on the use of intercept material as evidence:

—Tere have been five Home Office reviews of this issue, some of which were overseen by the Leader of the Opposition when he was Home Secretary, and if we felt that there was an easy answer to it, we would want to pursue it. All of us want measures that enable us to convict criminals. We have offered the Leader of the Opposition and the leader of the Liberal Democrats, under Privy Council rules, the opportunity to meet the Prime Minister to discuss these issues…."[28]

5.51 The UK Government has, to date, resisted any change to the law that prohibits the use of intercepted telecommunications in court as evidence as set out in section 17 of RIPA.

The options for admissibility

5.52 Realistically, there are three options for the admissibility as evidence of material obtained through covert surveillance and interception of communications:

- All material inadmissible, whether from intercepts or covert surveillance

[27] House of Commons Hansard Debates for 7 February 2005, col 1232.
[28] Cited above, col 1241.

- All material admissible, whether from intercepts or covert surveillance.

- Material from intercepts inadmissible; material from covert surveillance admissible

The fourth possibility, that covert surveillance material should be inadmissible, but intercepts should be admissible, does not merit serious attention.

Option 1: Both intercepted and surveillance materials inadmissible

Arguments in favour of option 1

5.53 This option would be consistent with the recommendation in the consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*. The arguments in favour of such an approach include the following:

(a) It would avoid the risk of revealing the surveillance/interception capability of the law enforcement agencies.

(b) It would enhance privacy protection, by limiting the dissemination of surveillance/interception material through the prosecution process.

(c) While allowing the use of surveillance/intercept material as evidence might have a beneficial impact on the number of successful prosecutions in the short term, any such effect would dissipate as the surveillance/interception capability became known.

Arguments against option 1

5.54 The arguments against the first option include:

(a) Other than the Republic of Ireland and the United Kingdom, no comparable jurisdiction has such a complete ban on the use of surveillance/interception materials as evidence (and the United Kingdom allows surveillance material to be admitted as evidence).

(b) Even though surveillance/interception material could be used for intelligence purposes, it would have an adverse affect on the prosecution of offences if this material was inadmissible in every case.

(c) There may be circumstances where surveillance/interception materials would provide evidence of assistance to the defence.

Option 2: Both intercepted and surveillance materials admissible

Arguments in favour of option 2

5.55 This option reflects the current law in Hong Kong (though intercept material is, in practice, not used in evidence) and is the approach followed in all major jurisdictions save the United Kingdom and the Republic of Ireland. The arguments in its favour include:

(a) It enables all relevant and probative evidence to be made available in order to assist in the apprehension and conviction of criminals and to ensure a fair trial.

(b) It is consistent with the general principle that, in law, all relevant evidence is *prima facie* admissible evidence.

(c) The United Kingdom and the Republic of Ireland are alone among comparable jurisdictions in rendering materials from interceptions inadmissible. The law enforcement agencies in jurisdictions such as the US, Canada, Australia and New Zealand have apparently been able to operate on the basis of full admissibility without their surveillance/interception capabilities being compromised.

(d) It offers flexibility. There is no obligation to disclose such evidence until a decision has been made to prosecute. If disclosure would prove detrimental to law enforcement capabilities, then the prosecution may opt not to take the case further.

Arguments against option 2

5.56 The arguments against option 2 include:

(a) It would increase the risk of revealing the surveillance/interception capability of the law enforcement agencies.

(b) It would adversely impact on privacy by entailing the public dissemination of personal information.

(c) Making all potentially relevant material public (including unused material) could undermine public interests if this revealed intelligence sources or techniques and so impaired the ability to gather intelligence.

Option 3: Intercepted material inadmissible and covert surveillance material admissible

Arguments in favour of option 3

5.57 This option is the approach adopted in the United Kingdom under RIPA. The arguments in favour of this option include:

(a) It would avoid the risk of revealing the interception capability of the law enforcement agencies, while still allowing the use of material gained through covert surveillance.

(b) It would enhance privacy protection, by limiting the dissemination of interception material through the prosecution process.

(c) While allowing the use of intercept material as evidence might have a beneficial impact on the number of successful prosecutions in the short term, any such effect might dissipate as the surveillance/interception capability became known.

Arguments against option 3

5.58 The arguments against option 3 include the following:

(a) Other than the Republic of Ireland and the United Kingdom, no comparable jurisdiction has such a complete ban on the use of interception materials as evidence.

(b) Even though interception material could be used for intelligence purposes, it would have an adverse affect on the prosecution of offences if this material was inadmissible in every case.

(c) There may be circumstances where interception materials would provide evidence of assistance to the defence.

5.59 A particular issue which arises in relation to option 3 is whether there is a valid basis for treating differently the admissibility of the two classes of materials. The following arguments can be made in favour of such a distinction:

(a) The interception of communications involves a third party (the telecommunications service provider) while covert surveillance does not. In practical terms, the service provider may be less willing to cooperate with the law enforcement agencies if material obtained through interception is made generally admissible, than where such material is not available in court. If intercept material is admissible, the service provider will become part of the “chain of evidence” in respect of that material.

(b) The use of bugs and other surveillance techniques is relatively well-known, but the details of interception capability are not. There is therefore a greater risk of compromising law enforcement agencies‟ capabilities through the admission of material from intercepts than from surveillance.

(c) Interception of communications relates to a telephone number, rather than an individual, and is therefore less targeted than surveillance. Interception has greater potential to catch collateral material relating to innocent third parties (such as other persons using the intercepted telephone).

5.60 In response, it can be said:

(a) Covert surveillance may in some circumstances involve a third party (such as the proprietor of a hotel).

(b) It is difficult to justify a distinction which means that evidence of a telephone conversation will be admissible if it was obtained by a bug by the phone, but not if it was obtained by interception (as illustrated in the case of *R v E* referred to earlier in this Chapter).

(c) There is no basis for the assertion that surveillance capability is more, or less, well-known than that in respect of interception.

(d) There is no clear distinction between interception of communications and surveillance as regards the degree to which each is, or is not, targeted. An intercept of a phone will catch any person using that number but, in the case of a mobile phone, calls will usually only be made by and to one person. Equally, surveillance may involve numerous third parties, such as where a watch is kept on those entering or leaving particular premises.

Conclusions in respect of the admissibility of surveillance materials

5.61 Arguments for and against the admissibility of intercepted materials are finely balanced. On the other hand, the case for admissibility of surveillance materials has been more clearly made out. The majority of those responding to the Privacy Sub-committee‟s consultation paper (admittedly, now ten years ago) supported the use of materials obtained through covert

surveillance as evidence to assist in the apprehension and prosecution of criminals.[29]

5.62 The laws of the United States,[30] Canada,[31] and Australia[32] all countenance the admission as evidence of materials obtained by means of surveillance or through interception of communications. In the United Kingdom,[33] materials obtained through covert surveillance may now be used in evidence in criminal proceedings, subject to a judicial discretion to exclude evidence to secure a fair trial.[34]

5.63 Additional considerations weighing in favour of admissibility include the fact that if material obtained as a result of covert surveillance were inadmissible, it would mean that, even if that material was the sole evidence of a serious offence, that evidence could not be adduced. Similarly, evidence which might assist an accused could not be adduced if it was obtained by surveillance, even though the surveillance was authorised by the court.

5.64 Every accused has the right to a fair trial, and the obligation on the prosecutor to make fair disclosure to the defence is an integral part of a fair trial. If the prosecutor is possessed of material which may be of relevance to the defence, whether documentary or otherwise, this should be disclosed.[35] A prohibition on the use of surveillance materials as evidence and their

---

29 For instance, the Bar Association found it unsatisfactory that lawfully obtained material could not be used at trial. They preferred a regime which would allow the prosecution to decide whether, and to what extent, material obtained pursuant to a warrant is retained and used.

30 *Wiretap Act*, sections 2525 and 2518(9) and (10). The contents of any wire, oral or electronic communication intercepted or evidence derived therefrom may be received in evidence if each party has been furnished with a copy of the authorisation and the accompanying application not less than 10 days before the legal proceeding. An aggrieved person may move to suppress the contents of any intercepted communication on the grounds that: the communication was unlawfully intercepted; the authorisation was insufficient on its face; or the interception was not made in conformity with the authorisation. If the motion is granted by the judge, the contents of the intercepted wire or oral communication or evidence derived form it shall be treated as having been obtained in violation of the Act and shall not be received in evidence.

31 *Criminal Code*, section 189(5). Notice of intention to introduce evidence of lawfully intercepted communications, including those obtained pursuant to an authorisation, must be given to the accused together with a transcript of the private communication or a statement setting out its full particulars; and a statement of the time, place, dates of the private communication and the parties thereto, if known.

32 *Surveillance Devices Act 2004*, section 45(5). Information obtained from surveillance may be admitted into evidence for the investigation of a relevant offence; the making of a decision whether or not to prosecute a relevant offence and in relevant proceeding.

33 *Covert Surveillance: Code of Practice* issued pursuant to section 71 of the *Regulation of Investigatory Powers Act,* para 1.8: "*Material obtained through covert surveillance may be used in evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1984.*"

34 Section 78 of the *Police and Criminal Evidence Act 1984*. Section 78(1) provides: "*In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.*"

35 Para 18.1 of "*The Statement of Prosecution Policy and Practice"* issued by the Department of Justice, as revised in July 2005, and see section 18 generally on the duty of disclosure. Para 18.9 states: "*In deciding whether to provide copies of audio and video surveillance to the defence the prosecution are entitled to take into consideration the protection of the safety of an undercover police officer (R v Crown Prosecution Service and Another, Ex parte J and Another TLR 8 July 1999*)".

subsequent destruction would deprive the defence of the use of materials that might assist in the preparation of the defence case.[36]

5.65 Under the jurisprudence of the European Court of Human Rights, the admissibility of evidence is primarily a matter for regulation under domestic law.[37] The Court"s function is to determine whether the proceedings in question, taken as a whole, were fair, and whether the rights of the defence were adequately respected.[38] The interest of the community in securing relevant evidence of the commission of serious crime so that justice can be done is to be weighed against the interest of the individual who has been exposed to an illegal invasion of his fundamental right. Compliance with the right of fair hearing does not require the automatic exclusion of evidence obtained by covert means. What is required is that an accused should be entitled to an opportunity to challenge its use in evidence and to a judicial assessment of the effect of its admission upon the fairness of the proceedings.[39]

5.66 The test of admissibility of evidence in Hong Kong is currently governed by common law principles under which all relevant and probative

---

[36] Article 14(3)(b) of the International Covenant on Civil and Political Rights (ICCPR) as incorporated in Article 11(2)(b) of the Hong Kong Bill of Rights (HKBOR) provides that: "*In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality-including…(b) to have adequate…facilities for the preparation of his defence…".* In *Jespers v Belgium* (1981) 17 D.R. 61, at 87-88, it was held by the European Commission on Human Rights that "*the ‗facilities' which everyone charged with a criminal offence should enjoy include the opportunity to acquaint himself, for the purpose of preparing his defence, with the results of investigations carried out throughout the proceedings…. Any investigation [the prosecution] causes to be carried out in connection with criminal proceedings and the findings thereof consequently form part of the ‗facilities' within the meaning of Article 6 paragraph 3(b) of the Convention… In short, Article 6 paragraph 3(b) [of the European Convention on Human Rights which is equivalent to Article 14(3)(b) of the ICCPR and Article 11(2)(b) of the HKBOR] recognises the right of the accused to have at his disposal, for the purposes of exonerating himself or of obtaining a reduction in his sentence, all relevant elements that have been or could be collected by the competent authorities….*"

[37] In *Schenk v Switzerland* (1991) 13 EHRR 242, it was held by the European Court of Human Rights that: "*While Article 6 of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law. The court cannot therefore exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible.*"

[38] In *Khan v United Kingdom*, 8 BHRC 310, the European Court of Human Rights held that the admission of evidence obtained by means of a listening device in breach of Article 8 (on right of respect to private life) of the European Convention on Human Rights did not render the proceedings unfair, despite the fact that the prosecution case rested entirely on the disputed tape recording. It was held by the Court, at paras 34 and 39, that: "*It is not the role of the court to determine, as a matter of principle, whether particular types of evidence – for example, unlawfully obtained evidence – may be admissible or, indeed, whether the applicant was guilty or not. The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. This involves an examination of the ‗unlawfulness' in question and, where violation of another Convention right is concerned, the nature of the violation found…. The court would add that it is clear that, had the domestic courts been of the view that the admission of the evidence would have given rise to substantive unfairness, they would have had a discretion to exclude it under section 78 of the [Police and Criminal Evidence] Act.*"

[39] In *R v P* [2001] AC 146. The House of Lords (per Lord Hobhouse, at 161) stated that: "*It should be noted that the [European] court again emphasised that the defendant is not entitled to have the unlawfully obtained evidence excluded simply because it has been so obtained. What he is entitled to is an opportunity to challenge its use and admission in evidence, and a judicial assessment of the effect of its admission upon the fairness of the trial, as is provided for by section 78 [of the Police and Criminal Evidence Act 1984].*

evidence is admissible subject to a judicial discretion to exclude evidence where its prejudicial effect exceeds its probative value.[40] The test of admissibility is not whether the evidence has been obtained unfairly but whether its use as evidence against the accused at trial is unfair.[41]

5.67 A recent decision by the District Court of Hong Kong suggested that the installation of covert surveillance devices by the Independent Commission Against Corruption in the absence of proper legal procedures was in breach of Article 30 of the Basic Law (which guarantees the privacy of communications of Hong Kong residents) and was therefore unlawful.[42] However, the two recordings obtained through this covert surveillance were admitted into evidence as the court did not find any unfairness in their use against the accused in the trial and the court took the view that those who obtained the evidence had made a *bona fide* mistake as to their powers in that case.[43]

5.68 Having taken into account these various considerations, we recommend that materials obtained lawfully through covert surveillance carried out pursuant to a warrant or authorisation should be admissible as evidence in court. However, an accused should be entitled to an opportunity to challenge the use and admission of the surveillance materials in evidence and to a judicial assessment of the effect of the admission of that evidence

---

40 *R v Sang* [1980] AC 402, at 432-3.

41 It was held by the Court of Final Appeal in *Secretary for Justice v Lam Tat Ming* [2000] 2 HKC 693, at 706, that: *"The first limb of the test of evidence having been obtained unfairly is inappropriate and should be discarded. The test should only be that in the second limb, whether its use in evidence against the accused at his trial would be unfair. And unfairness is to be judged against what is required to secure a fair trial for him."*

42 *HKSAR v Li Man Tak* DCCC 689/2004, judgement dated 22 April 2005 by District Court Judge Sweeney. The prosecution sought to adduce into evidence visual and oral surveillance tapes made covertly of two meetings. The first meeting took place at a restaurant inside a hotel. The prosecution sought to produce a filmed recording of the outside of the VIP room at the restaurant to show persons entering and leaving the hotel and a recording of conversations inside that room made by way of listening or "bugging" devices. The second meeting took place at another restaurant where video film and sound recordings were made of the meeting by way of a video camera placed in a nearby table. None of the persons participating in either of those conversations was aware that they were being recorded. The court accepted that the offences then under investigation by the ICAC, namely, conspiracy to offer advantages to an agent, were serious offences. Although the two restaurants in question were public places, the court took the view that Article 30 was clearly designed to protect privacy of communication rather than privacy of venue. The court noted that the whole authorisation process was carried out without reference to any outside body and allowed of no right of inspection or appeal. There was no legislative framework to regulate covert surveillance. The court came to the view that there was a legislative *lacuna* and concluded that the process by which the surveillance was authorised was not "*in accordance with legal procedures*". The court suggested that a warrant should be required for conducting covert surveillance before law enforcement officers could invade the privacy of personal communications.

43 The court in *Li Man Tak*, above, at para 65, adopted the common law exclusionary approach to the evidence and came to the view that it could not find any unfairness in admitting those two recordings into evidence despite the fact that they were unlawfully obtained. However, Judge Sweeney, as he then was, pointed out that "*recent English authorities and commentary thereon show that the discretion to exclude evidence obtained unlawfully will generally not be exercised if those who obtained the evidence made a bona fide mistake as to their powers. By contrast, the discretion is generally exercised against the prosecution if the police acted mala fide, ie knowingly exceeding their powers. Now that a Hong Kong court has made a ruling that the installation of covert surveillance devices is in breach of the Basic Law without proper legal procedures in place, it may well be held in future criminal trials that the ICAC are acting mala fide if they continue this practice without some legislative basis.*"

upon the fairness of the trial. Whether material obtained by authorised covert surveillance is admissible in any proceedings should depend on whether its use in evidence against the accused would be fair.

5.69 Where materials have been obtained through unlawful covert surveillance as a result of a contravention of the statutory requirements relating to the issue of warrants or authorisations, we recommend that the materials should not be excluded simply on the ground of their having been obtained unlawfully. We take the view that such evidence may still be admissible if, having regard to all the circumstances, including whether the materials had been obtained lawfully, it appears to the court that the admission of such evidence would not have an adverse effect on the fairness of the proceedings.

5.70 We further recommend that where the surveillance materials have been obtained so unfairly as to constitute an affront to public conscience and to seriously undermine public confidence in the administration of justice, these would be sufficient grounds to justify the exclusion of such materials as evidence, even though it is not shown that the accused could not have a fair trial.[44]

---

[44] In *HKSAR v Shum Chiu and others* DCCC 687/2004, (ruling of Judge Livesey on 5 July 2005), four defendants (D1, D2, D3 and D6) were charged with the offence of conspiracy to offer advantages to a public officer. Applications were made on their behalf for a permanent stay of proceedings. The facts of the case were that a prosecution witness (PW1) acted as an undercover agent for the ICAC from May 2002 to June 2003. In November 2002, PW1 informed the ICAC that he was to attend a lunch with D3 and a lawyer on 16 November. The ICAC then arranged for PW1 to be equipped with a covert recording device so that the meeting could be recorded. PW1 attended the meeting at a restaurant at which D3 and two solicitors were present. The meeting lasted about an hour and was recorded by the ICAC using the covert recording device carried by PW1. The court pointed out in paragraph 30 of the judgment that the right to privacy is guaranteed by Articles 29 and 30 of the Basic Law and the right to receive confidential legal advice is enshrined in Article 35. It was held that there was a "cynical" and "flagrant" infringement of D3's right to legal professional privilege as it was unnecessary to make such covert recordings of the conversations between D3 and his solicitors since the ICAC already had sufficient evidence from other sources. The court stated that the covert recording by the ICAC of conversations which it knew would be likely to be subject to legal professional privilege would by itself, constitute "*a breach of a fundamental condition upon which the administration of justice as a whole rests*". The court accepted that this amounted to "*an affront to the public conscience with severe consequences for public confidence in the administration of justice*". An order for stay was made in respect of the criminal proceedings against all four defendants. An application for judicial review of the decision of Judge Livesey was made by the Secretary for Justice with judgment delivered by Hartmann J on 22 December 2005 in *Secretary for Justice v Shum Chiu and others* HCAL 101/2005. It was held by Hartmann J that the matter would have to be remitted to the District Court for a fresh determination in accordance with law. The reason for his decision is stated at paras 131 and 132 of his judgment: "*It is fundamental, I think, that the rules of fairness dictate that when any person, or group of persons, is accused in legal proceedings of a grave, indeed shameful, act which is said to amount to an abuse of the system of justice, that person, or those persons, must be given a full opportunity to answer the accusation. That principle is to be applied equally to officers of investigating agencies. Unless they are given that opportunity, leaving aside justice being done to them as individuals, how else can the court weigh the public interest in bringing the defendants to trial against the public interest in ensuring that officers of investigating agencies do not themselves flout the law?...I have been drawn to the conclusion that the refusal by the trial judge to allow prosecuting counsel to resile from his earlier concessions acted to prevent the court from conducting the searching inquiry which it was obliged to conduct. I find it difficult, for example, to see how the court could determine whether the ICAC had or had not acted in bad faith – a consideration of central importance – without allowing officers of the ICAC to explain their position."* At paras 36 to 38 of his judgment, Hartmann J explained the principles to be applied in determining an application for a

5.71 It follows from our conclusion in respect of the admissibility of covert surveillance materials that we reject the first of the three options set out at paragraph 5.52 above. We defer further discussion of the second and third option until the next Chapter, where we consider the related issue of the retention and destruction of materials obtained through covert surveillance.

---

permanent stay of proceedings: "*The principles to be applied in determining an application for a permanent stay of proceedings have been comprehensively considered and determined in two judgments of the Court of Final Appeal (the CFA'), both arising out of the same set of criminal proceedings. The judgments are HKSAR v Lee Ming Tee & Another (2001) 4 HKCFAR 133 and HKSAR v Lee Ming Tee and Securities and Futures Commission (2003) 6 HKCFAR 336. In the first Lee Ming Tee judgment, the CFA confirmed that a stay would only be ordered in exceptional cases'. It was, said the court, a jurisdiction to be only most sparingly exercised. In respect of the first limb, the CFA said that a stay would be granted if, notwithstanding the range of remedial measures available at the trial, a fair trial for the accused is found to be impossible and continuing the prosecution would amount to an abuse of process'. In respect of this first limb, the court said that:"(i) In determining whether a fair trial was possible, a court should look to whether fairness is achievable in practical and not absolute terms. (ii) The power to ensure a fair trial is not simply a power to stop a trial before it starts. It is instead a power to mould the procedures of the trial to avoid or minimize prejudice. As Brennan J said in Jago v District Court of New South Wales (1989) 168 CLR 23, at 47: When an obstacle to a fair trial is encountered, the responsibility cast on a trial judge to avoid unfairness to either party but particularly to the accused is burdensome, but the responsibility is not discharged by refusing to exercise the jurisdiction to hear and determine the issues. The responsibility is discharged by controlling the procedures of the trial by adjournments or other interlocutory orders, by rulings on evidence and, especially, by directions to the jury designed to counteract any prejudice which the accused might otherwise suffer.'"* On the issue of whether a stay should be granted even though the fairness of the trial was not in question, Hartmann J referred at paras 39 to 41 of his judgment to the decision of the Court of Final Appeal in *HKSAR v Lee Ming Tee & Another* (2001) 4 HKCFAR 133 and stated: "*In respect of the second limb, the CFA referred to those rare cases' where, although the fairness of the trial was not in question, the Court granted a stay because the circumstances involved an abuse of power which so offended the Court's sense of justice and propriety that the entire prosecution was tainted as an abuse of process. The CFA emphasised that a stay under the second limb is not to be employed as a disciplinary measure; for example, in order to express a court's disapproval of official conduct. As the court said: The public interest lies in the guilt or innocence of the accused being fairly and openly determined at trial. For this to be displaced, powerful reasons must exist for concluding that such a trial, although fair, would nonetheless constitute an intolerable abuse of the court's process. The instances where such an argument has any prospects of success must necessarily be very rare.' As to the principles to be applied in considering an application under the second limb, these were more fully considered in the second Lee Ming Tee judgment. In this second judgment, the CFA (per Sir Anthony Mason NPJ) adopted the principles stated by Lord Steyn in R v Latif [1996] 1 WLR 104: In this case the issue is whether, despite the fact that a fair trial was possible, the judge ought to have stayed the criminal proceedings on broader considerations of the integrity of the criminal justice system. The law is settled. Weighing countervailing considerations of policy and justice, it is for the judge in the exercise of his discretion to decide whether there has been an abuse of process which amounts to an affront to the public conscience and requires the criminal proceedings to be stayed: R v Horseferry Road Magistrates' Court, ex parte Bennett [1994] 1 A.C. 42'"*

Chapter 6

Disposal of materials obtained from covert surveillance

6.1 As was explained at the start of Chapter 5, the question of admissibility of materials obtained through covert surveillance is closely related to the issue of whether such materials should be retained or destroyed. This Chapter looks at the question of retention and destruction of surveillance materials. As with Chapter 5, this Chapter also refers to interception of communications where that is relevant. The Chapter begins by setting out background information on retention and destruction of materials in the United Kingdom and Hong Kong, before considering the options available.

Background information: United Kingdom

Interception of communications

Interception of Communications Act 1985

6.2 Section 6 of the *Interception of Communications Act 1985* required the Secretary of State to make arrangements to ensure the minimum disclosure of any intercepted material. Section 6(3) of the 1985 Act further provided that this requirement would be satisfied in relation to any intercepted material "*if each copy made of any intercepted material is destroyed as soon as its retention is no longer necessary.*"

6.3 Section 2(2)(b) of the 1985 Act provided that an interception warrant could be issued "*for the purpose of preventing or detecting serious crime*": The House of Lords made clear in *R v Preston*[1] that preventing and detecting crime did not include the prosecution of crime. This means that under the *Interception of Communications Act 1985*, relevant material obtained by interception of telecommunications should not be retained for any pending or anticipated criminal prosecution since the prosecution of crime was not one of the purposes for which the warrant was issued in the first place.

---

1 [1994] 2 AC 130.

The Regulation of Investigatory Powers Act 2000

6.4 Part 1, Chapter 1, of RIPA replaces the *Interception of Communications Act 1985* and provides a regulatory system for the interception of communications in the course of their transmission.

6.5 Section 15(3) of RIPA provides for the destruction of any intercepted material and any related communication data as soon as they are no longer necessary for any of the authorised purposes specified in section 15(4). Section 15(3) and (4) reads:

> *"(3) The requirements of this subsection are satisfied in relation to the interception of material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.*
>
> *(4) For the purposes of this section something is necessary for the authorised purposes if, and only if --*
>
> *(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);*[2]
>
> *(b) it is necessary for facilitating the carrying out of any functions under this Chapter of the Secretary of State;*
>
> *(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Interception of Communications Commissioner or of the Tribunal;*
>
> *(d) it is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or*
>
> *(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923."*

[2] Section 5(3) of RIPA provides: "*…a warrant is necessary on grounds falling within this subsection if it is necessary - (a) in the interest of national security; (b) of the purpose of preventing or detecting serious crime; (c) for the purpose of safeguarding the economic well-being of the United Kingdom; or (d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.*"

6.6 The actual operation of section 15(3) of the Act is further explained in paragraph 6.8 of the *Interception of Communications: Code of Practice*, which states:

> *—6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the jurisdiction for its retention is still valid under section 15(3) of the Act."*

6.7 Section 17 of RIPA prohibits intercepted materials from being adduced as evidence either by the prosecution or the defence in legal proceedings. Section 18 provides limited exceptions to the general rule under section 17.

6.8 Paragraphs 7.3 and 7.4 of the *Interception of Communications: Code of Practice* explain the meaning of section 17 of RIPA*:*

> *—7.3 The general rule is that neither the possibility of interception nor intercepted material itself plays any part in legal proceedings. This rule is set out in section 17 of the Act, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Act (or the Interception of Communications Act 1985). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves 'equality of arms' which is a requirement under Article 6 of the European Convention on Human Rights.*
>
> *7.4 Section 18 contains a number of tightly-drawn exceptions to this rule. This part of the Code deals only with the exception in subsections (7) to (11)."*

6.9 Section 18(7)(a) of RIPA permits disclosure of intercepted material that continues to be available to "a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him by his duty to secure the fairness of the prosecution" which is apparently in contradiction with what is envisaged under section 17 of the Act, namely that intercepted material is not generally admissible as evidence in legal proceedings.

6.10 Paragraphs 7.5 to 7.7 of the *Interception of Communications: Code of Practice* state the rationale and explain the operation of section 18(7)(a) of RIPA:

> *—7.5 Section 18(7)(a) provides that intercepted material obtained by means of a warrant and which continues to*

be available, may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.

7.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of him by his duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he is given access under section 18(7)(a) to mount a cross-examination, or to do anything other than to ensure the fairness of the proceedings.

7.7 ***The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is, still, for the intercepted material to be destroyed in accordance with the general safeguards provided by section 15. The exceptions only come into play if such material has, in fact, been retained for an authorised purpose. Because the authorised purpose, given in section 5(3)(b) („for the purpose of preventing or detecting serious crime") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the section 15(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.*** *[emphasis added]*

7.8 Be that as it may, section 18(7)(a) recognises the duty on prosecutors, acknowledged by common law, to review all available material to make sure that the prosecution is not proceeding unfairly. „Available material" will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorised purpose.

7.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of the holder of this material the prosecutor should be informed that a warrant has been issued under section 5 and that material of possible relevance to the case has been intercepted.

7.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, he will decide how the prosecution, if it proceeds, should be presented."

6.11 There is no duty of retention by Communication Service Providers of communications data under RIPA.

Covert surveillance

RIPA

6.12 The retention and destruction of material obtained through the use of covert surveillance is provided for under paragraphs 2.16 and 2.17 of the *Covert Surveillance: Code of Practice* issued under RIPA:

> *"2.16 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.*
>
> *2.17 In the cases of the law enforcement agencies (not including the Royal Navy Regulating Branch, the Royal Military Police and the Royal Air Force Police), particular attention is drawn to the requirements of the code of practice issued under the Criminal and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained."*

6.13 Unlike the requirements for intercepted materials, there is no statutory prohibition against use of covert surveillance materials as evidence. On the contrary, as stated in paragraphs 2.16 and 2.17 of the *Covert Surveillance: Code of Practice,* the general rule is that materials obtained through covert surveillance should be retained if they may be of relevance to pending criminal or civil proceedings.

6.14 Section 81(5) of RIPA specifically makes provision to include the gathering of evidence for use in legal proceedings as part of the meaning of the detection of serious crime. However, section 81(5) also expressly provides that such definition does not apply to Part 1, Chapter 1 of the Act, which deals with the interception of communications. This clearly marks the distinction between the use of materials obtained through interception of communications and those by means of covert surveillance:

6.15 Section 81(5) of RIPA reads:

> *"(5) For the purpose of this Act detecting crime shall be taken to include -*

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed;

and any reference in this Act to preventing or detecting serious crime shall be construed accordingly, except that, in Chapter 1 of Part 1 [on Interception of Communications] it shall not include a reference to gathering evidence for use in any legal proceedings."

The Criminal Procedure and Investigations Act 1996

6.16 Section 3 of the *Criminal Procedure and Investigations Act 1996* (CPIA) requires the prosecutor to disclose material which in his opinion might undermine the case against the accused where an accused has been charged. However, there are two exceptions to this duty of disclosure, namely, where the material is subject to public interest immunity as set out in section 3(6) of the Act, or where disclosure is prohibited by section 17 of RIPA, as stipulated under section 3(7) of CPIA.

6.17 There is no statutory requirement under RIPA or CPIA to retain any relevant intercepted material for use in pending or future criminal proceedings. The duty of disclosure of any intercepted materials to the defence therefore generally does not arise as the materials would have already undergone destruction prior to reaching the stage of prosecution.

6.18 Paragraph 2.17 of the *Covert Surveillance: Code of Practice* issued under RIPA requires the law enforcement agencies to observe the relevant provisions governing the retention of materials under the Code of Practice issued under CPIA. The CPIA Code of Practice imposes a duty on the investigator to retain materials obtained in a criminal investigation which may be relevant to the investigation.[3] Paragraph 5.7 of the CPIA Code of Practice specifies clearly that materials relevant to criminal investigation should be retained until a decision is taken as to whether to a person should be charged with an offence, in which case it should be kept until the person is acquitted or convicted:

[3] Para 2.1 of the *Code of Practice* under CPIA defines "*criminal investigation*" as "*an investigation conducted by police officers with a view to it being ascertained whether a person should be charged with an offence, or whether a person charged with an offence is guilty of it. This will include: investigations into crimes that have been committed; investigations whose purpose is ascertain whether a crime has been committed, with a view to the possible institution of criminal proceedings; and investigations which begin in the belief that a crime may be committed, for example when the police keep premises or individuals under observation for a period of time, with a view to the possible institution of criminal proceedings.*"

—5.7 All material which may be relevant to the investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence.

5.8 If a criminal investigation results in proceedings being instituted, all material which may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case."

6.19 This reinforces the duty of the law enforcement agencies to retain materials obtained through covert surveillance where they may be used as evidence for pending or future criminal proceedings and until the conclusion of those proceedings.

6.20 There is a legal duty imposed on the law enforcement agencies under paragraph 2.18 of the *Covert Surveillance: Code of Practice* to ensure that arrangements exist for the handling, storage and destruction of material obtained through the use of covert surveillance under RIPA:

—Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material."

Code of Practice for Data Protection under the Data Protection Act 1998

6.21 Where no proceedings are to be instituted, personal information which forms part of the materials gathered during covert surveillance should be disposed of under the *Data Protection Act 1998.*

6.22 A Code of Practice for Data Protection was produced in October 2002 by the Association of Chief Police Officers ("the ACPO Code") to provide the Police Service with a set of guiding principles and procedures for compliance with the 1998 Act. The ACPO Code has been endorsed by the Information Commissioner pursuant to section 51(4)(b) of the *Data Protection Act 1998.*

6.23 Chapter 8 of the ACPO Code states the principle applying to the retention of personal information as follows:

—Personal information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

6.24 Paragraph 8.2 of the ACPO Code states that:

—Failure to remove data when their purpose has been served will result in inaccurate, irrelevant, excessive and out of date data being held. All of these would be breaches of the Data Protection Principles.

There may be occasions where information needs to be retained for longer period to fulfil statutory requirements, or other policing purposes.

In these cases a period beyond which the information may no longer be retained should be determined.

Consideration should be given to having all personal information removed. Within that period it may be possible to delete particular information when it is patently obvious that it will no longer be required.

In some cases it will be necessary for further enquiries to be made and/or the views of the officer responsible for the initial record to be sought before a decision to remove the information can be properly taken."

6.25 The guiding principle is that any personal information (including material collected through covert surveillance) is to be subject to periodic review and any personal information that is no longer required is to be removed from information collections. This would include information collected through covert surveillance which is not required for prosecution purposes.

Background information: Hong Kong

The consultation paper on Privacy: Regulating Surveillance and the Interception of Communications

6.26 The consultation paper considered how surveillance materials should be treated in order to meet privacy requirements and recommended the adoption of provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985 to ensure adequate safeguards for the retention of surveillance materials:[4]

—Section 6 of the United Kingdom Interception of Communications Act required that the Secretary of State shall make such arrangements as are necessary to ensure that:

- *the extent to which the material is disclosed*

[4] Consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*, paras 6.57 – 6.60.

- *the number of person 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.*[5]

6.27 The sub-committee set out the benefits of adopting provisions similar to section 6 of the 1985 Act as follows:

> *It became apparent during the trial in Preston (although no evidence was led to that effect) that the defendant's 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 inquires resulted in charges being laid, and it was this, rather than section 9's restrictions on admissibility …which precluded the defendants from having the material admitted.*
>
> *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*

[5] Consultation paper, para 6.57.

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. …"[6]

6.28 The sub-committee concluded in the consultation paper that surveillance materials should be destroyed immediately after their purpose has been spent in addressing the earlier stage of the fight against crime, namely prevention and detection. The fruits of authorised surveillance should never be available as evidence in a prosecution:

"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. …"[7]

6.29 In the light of its recommendation that surveillance materials should not be admissible as evidence, the sub-committee made no proposals in relation to disclosure of such materials.

The report on Privacy: Regulating the Interception of Communications

6.30 In its report on *Privacy: Regulating the Interception of Communications,* the Law Reform Commission maintained a similar view to that put forward by the Privacy Sub-committee in the consultation paper. The Commission recommended that intercepted materials should be inadmissible as evidence and should be destroyed once their functions had been fulfilled:

"The United Kingdom model provides a practical approach. The destruction of the intercepted material protects the privacy of targets and innocent persons who had contacts with them. There would be no question of making full disclosure of the contents of communications to other parties to the proceedings. The problems arising from the disclosure of unused material could therefore be avoided. Imposing a requirement that intercepted material should be destroyed would also boost public confidence in the warrant system. Furthermore, the

---

6 Consultation paper, paras 6.58 and 6.59.

7 Consultation paper, para 6.60.

secrecy of the manner in which the material was intercepted would not be compromised."[8]

6.31 The Commission pointed out, however, that the use of analyses compiled on the basis of the intercepted materials would be permissible:

> *"It has never been our intention to prohibit the retention and use of analyses compiled on the basis of primary materials obtained through authorised interception (i.e. the secondary material or the so-called 'fruits' of interceptions). Although the intercepted material (e.g. tapes and transcripts) would be destroyed under our proposals, the law enforcement agencies should be allowed to retain the analyses as intelligence in order to assist their investigations."*[9]

6.32 The Commission further recommended that in an application for a warrant authorising interception of telecommunications, the authorising judge should make such arrangements as he considers necessary to ensure that:

> *"(a) the extent to which the intercepted material is disclosed;*
>
> *(b) the number of persons to whom any of the intercepted material is disclosed;*
>
> *(c) the extent to which the intercepted material is copied; and*
>
> *(d) the number of copies made of any of the intercepted material*
>
> *is limited to the minimum that is necessary for the purpose for which the application was made. A transcript shall be treated as a copy of the intercepted material. This requirement will be satisfied if each copy made of any of the intercepted material is destroyed as soon as its retention is no longer necessary for the specified purpose."*[10]

The Interception of Communications Ordinance (Cap 532)

6.33 Section 7 of the *Interception of Communications Ordinance (Cap 532)* provides for the retention and destruction of intercepted materials under different circumstances depending on whether they may be used as evidence in future legal proceedings. Section 7 reads:

> *"(1) Where a court order has been terminated by the judge or has expired and has not been renewed, all intercepted*

---

8 Report on *Privacy: Regulating the Interception of Communications*, para 7.14.

9 Report on *Privacy: Regulating the Interception of Communications*, para 7.18

10 Report cited above, para 7.22

material obtained under that court order shall be placed in a packet and sealed by the authorized officer, and that packet shall be kept away from public access.

(2) Where a charge is laid against the person named in the court order, the authorized officer shall notify the judge who may order the release of the intercepted material to the prosecutor where the latter intends to tender the intercepted material as evidence in criminal proceedings.

(3) Where the prosecutor intends to tender the intercepted material as evidence in criminal proceedings, he shall notify the accused of this intention at least 10 days before the trial date and furnish him with-

(a) a copy of the application made under section 5;
(b) a copy of the court order;
(c) a copy of the application for renewal of the court order, if any.

(4) Any information obtained by an interception that, but for the interception, would have been privileged remains privileged and inadmissible as evidence without the consent of the person enjoying the privilege.

(5) Where no charge is laid against the person named in the court order within 90 days of the termination of a court order, the court shall inform the authorized officer of its intention to-

(a) destroy the intercepted material in the sealed packet; and
(b) notify the person named in the order that his communications have been intercepted,

and shall give the authorized officer 5 days to inform the court whether or not he wishes to challenge the court's intentions.

(6) Where the authorized officer wishes to challenge the court's intentions stated in subsection (5)(a) or (b), he shall in writing provide the judge with his reasons for opposing the court's said intentions and it shall remain within the judge's discretion whether or not to accept these reasons.

(7) Where -

(a) the authorized officer does not inform the court of his intention to challenge the court's intentions stated in subsection (5)(a) or (b) within 5 days; or

(b) after considering the authorized officer's reasons for preventing the court from carrying out its intentions, the court decides not to accept his reasons,

the court shall order that all intercepted material in the sealed packet be destroyed immediately and shall notify the person named in the order that his communications have been intercepted, providing in the notice details on-

(i) the type of communication that was intercepted;
(ii) the time and date of each interception; and
(iii) the reasons for conducting the interception.

(8) Where the judge exercises his discretion not to order the destruction of intercepted material, he may make an order to specify the period for which the intercepted material will remain undestroyed."

6.34 In summary, section 7 requires that, upon termination or expiry of a warrant, all intercepted material obtained is to be placed in a sealed packet. Where a charge is laid, the court may order the release of the intercepted material to the prosecutor. Notification is to be given to the accused of the intention by the prosecution to tender the intercepted material as evidence at least 10 days before the trial.

6.35 Where no charge is laid within 90 days of the termination of the warrant, the court must inform the authorised officer of the relevant law enforcement agency of its intention to destroy the intercepted material in the sealed packet. If the authorised officer objects to the destruction, he must inform the court of his reasons within five days of the notice from the court. If there is no challenge, or where the court does not accept the reasons offered, the court will order the immediate destruction of the intercepted material in the sealed packet.

6.36 Where the judge does not order the destruction of intercepted material, he may specify the period for which the intercepted material may be retained.

Executive Order No 1 of 2005

6.37 The Law Enforcement (Covert Surveillance Procedures) Order which came into operation on 6 August 2005 does not include any provision

on the admissibility or destruction of materials gathered from covert surveillance.

Security Bureau's Proposed Legislative Framework on Interception of Communications and Covert Surveillance

6. 38 In February 2006, the Security Bureau issued a paper entitled "*Proposed Legislative Framework on Interception of Communications and Covert Surveillance*". Paragraphs 32 to 35 of the paper set out the bureau‟s proposals for the "handling and destruction of materials‟ and "evidential use" of telecommunications intercepts and covert surveillance products. They read as follows:

> *~~-~~Handling and destruction of materials*
>
> *32. The legislation would require arrangements to be made to ensure that materials obtained by interception of communications and covert surveillance are properly handled and protected. These include keeping the number of persons who have access to the products of interception and surveillance and their disclosure to a minimum, and requiring that such products and any copies made are destroyed or otherwise disposed of as soon as their retention is no longer necessary.*
>
> *Evidential use*
>
> *33. We have for a long time adopted the policy of not using telecommunications intercepts as evidence in legal proceedings in order to, among other things, protect privacy. At the same time, intercepts are destroyed within a short time. This ensures the equality of arms between the prosecution and the defence as neither side may use intercepts as evidence. In addition, it minimizes the intrusion into privacy of innocent third parties through keeping the records which will be subject to disclosure during legal proceedings.*
>
> *34. On the other hand, covert surveillance products are used as evidence in criminal trials from time to time. As covert surveillance is usually more event and target specific, the impact on innocent third parties and hence privacy concerns are less.*
>
> *35. We propose that the current policy and practice in respect of evidential use above should be codified in law. The legislation should, therefore, expressly disallow all telecommunications intercept from evidential use in proceedings. As a corollary, such materials would not be*

made available to any party in any proceedings, and questions that may tend to suggest the occurrence of telecommunications interception should also be prohibited from being asked in such proceedings."

6.39 Security Bureau's proposals in respect of the use of intercepted materials and covert surveillance materials as evidence in legal proceedings basically follow the approach adopted by RIPA.

The "intelligence-gathering model" versus the "evidence-gathering model" – approaches to admissibility

6.40 In an article entitled *The Executive Order on Covert Surveillance: Legality Undercover?* by Simon M N Young[11], the author has categorised the alternative approaches to admissibility and the retention or destruction of materials gathered from covert surveillance as the "intelligence-gathering model" and the "evidence-gathering model". The advantages and disadvantages of the two models are analysed as follows:

—In the debate to enact legislation on covert surveillance discussions will likely focus on two contrasting models of implementation. The first model, which could be described as the —intelligence gathering model", imposes minimal hurdles on law enforcement at the authorisation stage. This results in a high volume of information gathered by covert surveillance, but law enforcement takes added precautions to protect the privacy of this information including the timely destruction of the recorded information. The information is treated as —intelligence" rather than as evidence in trial proceedings. The intercepted communication is kept private from the public but not from law enforcement.

The second model envisages the process as a means of gathering fruitful evidence to be admitted at trial. Thus this —evidence-gathering model" provides greater safeguards at the authorisation stage, which most likely will involve judicial authorisation. Law enforcement must also act responsibly when carrying out the surveillance since improper or unreasonable behaviour may jeopardise the admissibility of the evidence. The consequence is a smaller volume of information gathered but the advantage gained is that this information can be used as evidence and in most cases, it will be very strong evidence for the prosecution.

While it is true that the two models are not mutually exclusive, the second model offers a higher degree of protection for fundamental rights and freedoms. One should not be misled by

[11] 2005 HKLJ, Vol 35, Part 2, 265.

the privacy assurances of the intelligence-gathering model. Privacy interests are compromises from the moment the covert surveillance begins. The first model is already being practised by law enforcement in Hong Kong with authorisations granted under section 33 of the Telecommunications Ordinance (Cap 106). Unfortunately this experience has been marked by an aura of secrecy and overly broad claims of public interest immunity. The total lack of transparency has bred public cynicism in both the law enforcement agency and the government. The assurance that the intelligence gathered will not be used as evidence is also misleading because such intelligence can often lead to the finding of admissible evidence which would not otherwise have been found. Use of this derivative evidence allows law enforcement to realise the fruits of the evidence-gathering model without having to surpass the due process hurdles of that model. The policy to destroy surveillance information helps law enforcement to obfuscate the degree to which their evidence gathering has been aided by the intelligence obtained."[12]

6.41 The article concludes that the "evidence-gathering model" is to be preferred since it offers a higher degree of protection to the right of privacy. Similar arguments could be applied in favour of allowing the use of intercepted materials as evidence in court.

Relevant provisions in other jurisdictions

6.42 It is a criminal offence in Canada for a person to willfully use or disclose the content or the existence of a private communication intercepted by means of a device without the consent of either the originator or the intended recipient of the communication.[13]

6.43 In the United States, it is illegal to disclose the contents of wiretapped communications except when authorised under a court order or with the lawful consent of the originator or the intended recipient of such communication.[14] Immediately upon the expiration of the time period of the

---

12 Cited above, at 275.

13 Canadian *Criminal Code,* section 193(1). Any person who commits the offence would be liable to imprisonment for a term not exceeding two years. Under section 193(2) and (3), disclosure of a private communication would not constitute an offence if it was made in the course of or for the purpose of giving evidence in any civil or criminal proceedings; in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted; to comply with a notice of intention to produce evidence; to enable the Canadian Security Intelligence Services to perform its duties and functions; or where there was already prior disclosure as evidence in legal proceedings.

14 US *Wiretap Act*, section 2511(1)(c) and (e). Any violation of the relevant provision prohibiting disclosure would be liable to a fine or imprisonment for not more than five years, or both: section 2511(4)(a). Applications made and orders granted for wiretapping are sealed with their custody being directed by the judge. Such applications and orders are to be disclosed to the defendant only upon a showing of good cause, section 2518(8)(b).

warrant, or its extensions, the recordings must be made available to the judge issuing the warrant and sealed at his direction.[15]

6.44 It is an offence in Australia intentionally to use, record, communicate or publish "protected information" obtained from the use of surveillance devices except if it is obtained under a warrant, emergency authorisation or tracking device authorisation.[16] Safe keeping requirements for „protected information" are imposed on law enforcement agencies.[17] Records of protected information are to be destroyed as soon as practicable if they are not likely to be required for use in connection with civil or criminal proceedings.[18]

6.45 In the United Kingdom, material obtained through surveillance which could be relevant to pending or future criminal or civil proceedings must be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.[19] Material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.[20] Each public authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Material obtained from properly authorised surveillance may be used in other investigations.[21] A centrally retrievable record of all authorisations is to be held by each public authority and regularly updated whenever an authorisation is granted, renewed or cancelled.[22]

---

15 US *Wiretap Act*, section 2518(8)(a). The presence of the seal, or a satisfactory explanation for its absence, is a prerequisite to using or disclosing the contents of the recordings.

16 *Surveillance Devices Act 2004*, section 45. The maximum penalty is two years imprisonment. Where the use etc recklessly endangers health or safety or prejudices the conduct of an investigation into a relevant offence, the maximum penalty is 10 years imprisonment.

17 *Surveillance Devices Act 2004*, sections 51 to 52. Each law enforcement agency must keep records of applications made and warrants, emergency authorisations or tracking device authorisations issued; records containing the information required in the annual report to the Minister; and a register of warrants and authorisations that contains information such as the date the instrument was issued or refused, the name of the authorising judicial officer or other person, the name of the executing officer, the relevant offence, the period for which the instrument was in force and any variations or extensions of the warrant.

18 *Surveillance Devices Act 2004*, sections 46 and 47. The chief officer of a law enforcement agency is required to ensure that every record or report comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report. A person giving evidence may object to the disclosure of information that could reveal details of surveillance device technology or methods of use. In deciding whether to make a non-disclosure order a court must take account of whether disclosure is necessary for the fair trial of the defendant, or in the public interest.

19 *Covert Surveillance: Code of Practice*, para 2.16, issued under the *Regulation of Investigatory Powers Act 2000*.

20 *Covert Surveillance: Code of Practice*, para 2.17 referring to code of practice issued under the *Criminal Procedure and Investigations Act 1996*.

21 *Covert Surveillance: Code of Practice*, para 2.18. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

22 *Covert Surveillance: Code of Practice*, para 2.14. The record is to be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for a period of at least three years from the ending of the authorisation.

The options for retention and destruction of materials obtained through interception and covert surveillance

6.46 We set out at paragraph 5.52 of the previous Chapter the three options available for determining the admissibility as evidence of material obtained through covert surveillance and interception of communications:

- Option 1: All material inadmissible, whether from intercepts or covert surveillance
- Option 2: All material admissible, whether from intercepts or covert surveillance.
- Option 3: Material from intercepts inadmissible; material from covert surveillance admissible

6.47 We rejected the first of these options in the previous Chapter for the reasons set out there. Modifying the remaining two options now to incorporate the retention or destruction of surveillance/intercept materials, the options are:

- Option 2: All material admissible, whether from intercepts or covert surveillance; materials may be retained and must be disclosed to defence where there is a prosecution.
- Option 3: Material from intercepts inadmissible and automatically destroyed; material from covert surveillance admissible and retained.

Option 2: All evidence admissible; materials may be retained

6.48 Under this option, material from both interception of communications and covert surveillance would be admissible, subject to judicial discretion to exclude evidence to secure a fair trial.

6.49 A modification of this option, which would ensure greater privacy protection than the unmodified version, would be to provide that, while intercept materials should be admissible, the normal rule should be that intercepted materials and any copies of them should be destroyed within a specified period after the expiry of the warrant, unless the relevant law enforcement agency needs to retain them for use in pending or future legal proceedings or for other legitimate reasons. Where the law enforcement agency wishes to retain intercept materials, approval must be obtained either from the court or from the supervisory authority for their retention. If intercept material is retained for use in criminal proceedings then the normal rules on disclosure would require any relevant material to be made available to the defence.

6.50 Covert surveillance materials may be retained for a specified period, depending on whether they may be relevant for use in pending or future legal proceedings. Covert surveillance materials must be destroyed if they are no longer required for any legitimate purpose, including that of being used by the prosecution or the defence as evidence in subsequent proceedings. The procedures for the retention and destruction of materials are to be governed by guidelines approved by the supervisory authority.

6.51 The principles governing the retention and destruction of materials would be the same for intercepted materials and for covert surveillance materials, namely, that they are not to be retained longer than is necessary. However, the "default position" for telecommunication intercepts would be that they should be destroyed within a specified period after the expiry of the warrant unless their retention is necessary. Retention would only be permitted with the approval of the court or the supervisory authority.

6.52. This proposed difference of treatment between telecommunications intercepts and surveillance materials is because, firstly, it would not be appropriate to burden the telecommunications service providers with the duty of retaining a large volume of intercepts for a period beyond their normal business practice and, secondly, it would be difficult to control the dissemination of those materials as they would be kept by the service providers rather than the law enforcement agencies. In addition, telephone intercepts would only be used as evidence in exceptional cases, whereas covert surveillance materials would be likely to be used more widely in criminal prosecutions.

Arguments in favour of option 2

6.53 The arguments in favour of option 2, and against option 3, include the following:

(a) The argument that the use of intercepted telecommunications as evidence would expose the capabilities of the law enforcement authorities, thus allowing criminals to take more effective evasive action, is unconvincing. Jurisdictions such as the United States, Australia, New Zealand and Canada allow the admission of such evidence and experience no such difficulties. The United Kingdom and Ireland are alone in excluding this material.

(b) There are already adequate safeguards to ensure that sensitive information about the operational capability of law enforcement agencies would not be revealed if intercept material was made admissible:

(i) The doctrine of public interest immunity enables the prosecution to withhold material where the trial judge agrees that the public interest in non-disclosure

outweighs the defendant‟s interest in having full access to the intercepted materials;

(ii) Where large quantities of intercepts are not relevant to any issue relating to the case, the disclosure rules do not apply irrespective of any question of public interest immunity;

(iii) It is not uncommon in the criminal courts for sensitive information to be withheld, whether it is to preserve the anonymity of informers, or to protect police observation techniques, intelligence service reports or interception technology or methods.

(c) It is difficult to justify treating intercepted telecommunications and covert surveillance materials differently, since admitting evidence of either category of material would run the same risk of revealing law enforcement capabilities.

(d) It is illogical that a tape-recording obtained by means of a covert listening device is admissible in evidence but not admissible when it has been obtained by a telephone intercept, as shown in *R v E.*

(e) Under the Sub-committee‟s proposal, privacy risks would be mitigated by the fact that interception material would be destroyed within a specified time after the expiry of the warrant unless its retention was approved by the court or the supervisory authority.

Option 3: Intercepts inadmissible and to be destroyed; covert surveillance materials admissible and may be retained

6.54 This is the option proposed by the Security Bureau and currently adopted under the United Kingdom *Regulation of Investigatory Powers Act 2000*.

6.55 Telecommunication intercepts are prohibited from being used as evidence in legal proceedings. No questions that may tend to suggest the occurrence of telecommunications interception should be asked in such proceedings. The intercepts are to be destroyed within a short time.

6.56 However, covert surveillance materials are admissible as evidence in criminal proceedings. They may be retained for use in pending or future legal proceedings and destroyed only when their retention is no longer necessary.

6.57 The major difference between the second option and the third option (which is the UK system and the Security Bureau‟s proposal) is that

intercepted telecommunications are admissible as evidence under the former but not the latter. In addition, telecommunication intercepts are to be destroyed under the third option, irrespective of their relevance in subsequent legal proceedings.

Arguments in favour of option 3

6.58 The arguments in favour of option 3 (and against option 2) include the following:

(a) It minimises the intrusion into privacy of innocent third parties by avoiding the keeping of materials which may be subject to disclosure during legal proceedings. It also limits the risk that intercept material may be inadvertently or maliciously disseminated.

(b) The fact that materials obtained through interception cannot be used as evidence may provide a disincentive for law enforcement agencies to undertake interception in the first place.

(c) It ensures that the interception capabilities of law enforcement agencies are not exposed. Such exposure would run the risk that it would enable criminals to take more effective evasive action.

(d) It ensures "equality of arms" between defence and prosecution: neither side is able to use material obtained through interception of telecommunications as evidence.

(e) The difference in treatment of interception and surveillance materials reflects the different nature of the material obtained. Covert surveillance can be expected to be more event and target specific than interception of telecommunications. The impact on innocent third parties is less, and hence there are less privacy concerns.

Recommendations on retention, disclosure and destruction of materials obtained from covert surveillance

Internal guidelines for retention of personal information

6.59 We concluded in Chapter 5 for the reasons set out there that materials obtained through covert surveillance should be admissible as evidence. It is therefore necessary to make appropriate provision for the retention, disclosure and destruction of such materials. We recommend that the legislation regulating covert surveillance should require each law enforcement agency to ensure that systematic arrangements are in place for the handling, storage and destruction of material obtained through covert

surveillance. The legislation should also require each law enforcement agency to draw up internal guidelines (to be approved by the supervisory authority), setting out the policy and procedures for the disposal of surveillance materials.[23]

6.60 In formulating these internal guidelines, a balance must be struck between protecting the privacy rights of individuals whose personal information has been collected through covert surveillance and safeguarding the right to a fair hearing by ensuring that relevant materials are retained and made available to the defence. Prescribing a clear and ascertainable procedure for the management of the records relating to, and the materials obtained from, covert surveillance will not only provide standards for the agencies concerned but will help preserve the public"s confidence in the system.

6.61 We further recommend that materials obtained lawfully from covert surveillance by law enforcement agencies should be retained for a specified period in accordance with internal procedural guidelines.[24] Surveillance materials should not be kept for longer than is necessary for the achievement of the purpose for which they are to be used.[25] Appropriate measures should be taken to ensure that surveillance materials are protected against unauthorised or accidental access, processing, erasure or other use.[26]

6.62 The procedures must clearly specify the circumstances in which surveillance materials are to be destroyed. Records of information obtained by covert surveillance must be destroyed as soon as practicable if they are not likely to be required for use in connection with civil or criminal proceedings or if their retention is no longer necessary for the specified purpose.

6.63 A record of all applications for and the issue of warrants and internal authorisations should be held by each law enforcement agency and regularly updated.[27] As explained in later Chapters of this report, the law enforcement agencies will be required to make quarterly reports to the supervisory authority, and the authority will in turn be required annually to submit a report to the Legislative Council and a confidential report to the Chief

---

23 In the United Kingdom, the Association of Chief Police Officers (ACPO) has issued a detailed *Code of Practice for Data Protection*. It establishes procedures and safeguards to promote the maintenance of good practice and compliance with the *Data Protection Act 1998*. The introduction to the Code of Practice states (at page 6) that: "*As a large proportion of the data held in police information systems relates to individuals it is essential that a framework is established to ensure public confidence in the way police operate these systems. This Code of Practice is the means by which that framework is established and maintained*."

24 As specified under the *Code of Practice for Data Protection* issued by the ACPO in the UK, at para 8.2, it is not possible, in all instances, to lay down absolute rules about how long particular items of personal information which form part of a collection should be retained. However, such rules should be established where possible.

25 Data Protection Principle 2(2) under Schedule 1 of the *Personal Data (Privacy) Ordinance* (Cap 486). Procedures should be devised by law enforcement agencies to ensure that surveillance materials kept are periodically reviewed and materials that are no longer required must be destroyed. See para 8.1, *Code of Practice for Data Protection* issued by the ACPO in the UK.

26 Data Protection Principle 4 under Schedule 1 of the *Personal Data (Privacy) Ordinance* (Cap 486). See also para 10.1 of the *Code of Practice for Data Protection* issued by the ACPO in the UK relating to security of personal data kept by the police.

27 See Chapter 4 of this report on the procedure for authorisation, at paras 4.19 – 4.21.

Executive. There is no formal sanction proposed for a failure by a law enforcement agency to comply with the guidelines for the retention and destruction of material, but any such failure would be referred to in the supervisory authority"s report.

6.64 While we do not consider that there should be any restriction on a law enforcement agency passing *intelligence* obtained through covert surveillance to another law enforcement agency, we think that restrictions should be applied to the passing of *material* obtained through such surveillance. Reflecting the different level of intrusion involved in the respective types of surveillance, we recommend that where the surveillance was authorised by an internal authorisation, then material relating to any crime, no matter how minor, may be passed to another law enforcement agency. Where, on the other hand, the surveillance was authorised by a warrant, only material relating to a serious crime may be passed to another law enforcement agency. The logic behind this distinction is that the law enforcement agency would not have been able to obtain a warrant to undertake intrusive covert surveillance in respect of a minor crime, and it would therefore be wrong to allow collateral material relating to a minor crime which was uncovered during surveillance authorised by a warrant to be revealed to another law enforcement agency. Surveillance materials may only be passed to another law enforcement agency, and not to a third party, such as the Revenue Department.[28]

6.65 The supervisory authority should be consulted in difficult cases where there are uncertainties in relation to the application of any of these procedures.

Disclosure of surveillance materials.

6.66 We recommend that on an application for a warrant or internal authorisation authorising covert surveillance, the authorising judge or authorising officer should make such arrangements as he considers necessary to ensure that the disclosure of surveillance materials is limited to a necessary minimum. The judge or authorising officer should ensure that:

(a) the extent to which the surveillance material is disclosed;

(b) the number of persons to whom any of the surveillance material is disclosed;

---

[28] Data Protection Principle 3 under Schedule 1 of the *Personal Data (Privacy) Ordinance* (Cap 486) provides that personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than the purpose, or a directly related purpose, for which data were to be used at the time of their collection. However, section 58(2) of the Ordinance provides that an exemption to the application of Data Principle 3 applies where the use of the data is for the purposes of, *inter alia*, the prevention or detection of crime; the apprehension, prosecution or detention of offenders; or the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons.

(c) the extent to which the surveillance material is copied; and

(d) the number of copies made of any of the surveillance material

is limited to the minimum that is necessary for the purpose for which the application was made.

6.67 We further recommend that a person who intentionally discloses to any person the contents of any information obtained from authorised covert surveillance, knowing or having reasonable grounds to believe that the information has been obtained by covert surveillance, commits a criminal offence.

6.68 The proposed legislation should make provision for exceptions to the prohibition on disclosure of covert surveillance materials to third parties. These exceptions should include disclosure for the purpose of giving evidence in any legal proceedings; for preventing, investigating or detecting crime; for the purpose of safeguarding public security in respect of Hong Kong; or pursuant to an order of the court.

Conclusions in respect of materials obtained from interception of communications

6.69 he Commission"s 1996 report on *Privacy: Regulating the Interception of Communication*s recommended that materials obtained from the interception of communications should be inadmissible, regardless of their relevance. The proposals recently put forward by the Security Bureau adopt a similar approach, which echoes that followed by the United Kingdom. Although intercept material is legally admissible in Hong Kong, the long-standing practice is that it is not adduced in evidence and is destroyed. Of comparable jurisdictions, however, only Ireland and the United Kingdom render intercept evidence inadmissible: all others allow that evidence without apparent difficulty.

6.70 A modified option described at paragraphs 6.49 to 6.52 of this report would be that intercept material should be admissible, but that, in the absence of specific approval by the court or supervisory authority, such material should be destroyed within a specified period after the expiry of the warrant. That approach would give the prosecution the option of applying to retain intercept material. A concern with such an approach is its effect on the "equality of arms" between prosecution and defence: whether or not intercept material is available as evidence to prosecution or defence depends in the first instance on a decision by the prosecution as to whether or not to apply for approval to retain it. Equally, a difficulty with the existing practice, where all intercept material (though legally admissible) is automatically destroyed, is that material may be destroyed which might otherwise have assisted the defence.

6.71 In our view, the arguments in respect of the admissibility of materials obtained through the interception of telecommunications are finely balanced. We have not reached a clear conclusion, but by setting out the arguments in this report we hope to assist public discussion of this issue.

Chapter 7

Notification following termination of surveillance

Recommendations in the consultation paper

7.1 In its consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*, the sub-committee considered whether it was necessary to require that the object of surveillance be notified of the fact that he had been subject to surveillance.

7.2 The sub-committee‟s main concerns were that a requirement to notify the target or an innocent party of the fact that he had been the subject of surveillance once the surveillance had been discontinued would necessitate prolonged retention of surveillance materials. It would have considerable resource implications and might prejudice the purposes of the original intrusion. The sub-committee believed that accountability and control over the surveillance process could be directly and adequately addressed by the warrant system and the public reporting requirement.

7.3 The sub-committee therefore concluded in the consultation paper that a person who had been placed under surveillance need not be notified of the surveillance.

Review of previous recommendations

The responses to the consultation paper

7.4 Most of those who responded to the consultation paper were in favour of a requirement to give notification. This was because notification would enhance accountability; would enable an aggrieved individual to seek review against the issue and execution of the warrant or authorisation; would facilitate the use of surveillance materials in evidence; and would allow a person to challenge the admissibility of surveillance materials in legal proceedings.

Notification necessitated by revised recommendation on admissibility of evidence

7.5 In the consultation paper, the sub-committee considered that the privacy of the target would receive greater protection if all surveillance

materials were destroyed and rendered inadmissible in court without having to notify the target of that fact. Upon review, we take the view that materials obtained from surveillance should be admissible in evidence in legal proceedings against the accused, subject to a judicial discretion to exclude evidence in order to secure a fair trial. There is a general requirement that the prosecution must disclose its evidentiary material to the defence in advance of any trial, including material which the prosecution does not intend to adduce at trial but which might be of relevance to the defence. If surveillance materials are to be used in evidence, there will therefore be a duty on the prosecution to divulge the fact of surveillance to the defence once a prosecution is brought. In the light of this, it is therefore necessary to revise the previous recommendations on the requirement to give notification.

The basis of the notification requirement

7.6 In considering the notification requirement, we bear in mind the basis for a notification requirement, as set out in the consultation paper. First, it marks the seriousness of the earlier intrusion into privacy. The requirement would introduce an important element of accountability and deter the authorities from conducting surveillance unnecessarily.

7.7 Secondly, the individual should be able to challenge the grounds on which the intrusion was allowed. Denying the subject of surveillance such information would tend to undermine the efficacy of the mechanisms enhancing accountability, such as complaints procedures and the provision of compensation for wrongdoing. We also took the view that the public has a right to be told the extent to which intrusions were occurring.

Notification requirement under the Interception of Communications Ordinance (Cap 532)

7.8 We note that section 7 of the Interception of Communications Ordinance (Cap 532) requires notice to be given to the person whose communications have been intercepted.[1]

[1] Upon the expiry or termination of a court order, all intercepted material obtained under that court order must be placed in a packet, sealed by the authorised officer and kept away from public access. Where a charge is laid against the person named in the court order, the authorised office must notify the judge who may order the release of the intercepted material to the prosecutor. Where the prosecutor intends to tender the intercepted material as evidence in criminal proceedings, he is required to notify the accused of this intention at least 10 days before the trial dates and to supply the accused whose communications have been intercepted with a copy of the application for authorisation, a copy of the court order and a copy of the application for renewal, if any. Where no charge is laid against the person named in the court order within 90 days of the termination of the court order, the court must inform the authorised officer of its intention to destroy the sealed material and to notify the person named in the court order that his communications have been intercepted. The court must give the authorised officer five days to inform the court whether or not he wishes to challenge the court"s intented actions. The authorised officer may provide written reasons to the court for his challenge. Where the court doss not accept these reasons, or if no challenge is made by the aurhorised officer, the court will order that all intercepted material in the sealed packet be destroyed immediately and notify the person named in the order that his communications have been

Is subsequent notification to the target necessary?

7.9 We understand that the practice in Canada[2] and the United States[3] is to notify in writing the target of the interception within a specified period after authorisation has been granted, renewed or extended. Similar notification procedures have been adopted in Germany.[4] On the other hand, we note that there is no requirement of notification under the regulatory system for the interception of communications or covert surveillance in the United Kingdom.[5]

7.10 Under the European Convention jurisprudence, the lack of a mandatory requirement that the individual be notified of secret surveillance following the cessation of such conduct has not been found to be in violation of the right to privacy. The reasons stated by the European Court of Human Rights were that, as the activity or danger against which a particular series of surveillance measures was directed might continue for years after the suspension of those measures, subsequent notification to each individual

---

intercepted. The notice must provide details of the type of communication that was intercepted, the time and date of each interception, and the reasons for conducting the interception.

[2] Section 196(1), Part VI (Invasion of Privacy), *Criminal Code of Canada*. Notice is to be given to the person who is the object of the interception within 90 days after the period for which the authorisation was given or renewed. The judge may grant an extension or subsequent extension of the period for notification under section 196(2) to (5) of the Criminal Code for a total period not exceeding three years where he is satisfied that the investigation of an offence to which the authorisation relates, or a subsequent investigation of an offence of which an authorisation to intercept a private communication may be obtained, is continuing, or where the investigation is related to an offence committed in association with a criminal organisation or is a terrorism offence; and if the court is also of the opinion that the interests of justice warrants the granting of such application for extension.

[3] Section 2518(8)(d), US *Wiretap Act* requires the issuing or denying judge to cause an inventory to be served on the subject of a warrant within a reasonable time but not later than 90 days after the denial of or the termination of the period of the intercept order or the extensions thereof. The inventory is to include notice of the fact of the entry of the order or the application the date of the entry and the period of authorised, approved or disapproved interception, or the denial of the application; and the fact that during the period, wire, oral, or electronic communications were or were not intercepted. An inventory must be served on the persons named in the order or application and such other parties to the intercepted conversations as the judge may determine in his discretion in the interest of justice. The judge, upon filing of a motion, may in his discretion and in the interests of justice make available such portions of the intercepted communications, applications and orders to such persons (or their counsel) for inspection. The serving of the inventory may be postponed on an *ex parte* application for good cause shown.

[4] Under section 101(1) of the *Criminal Procedure Code* of Germany, individuals affected shall be notified of surveillance measures taken as soon as this can be done without endangering the purpose of the investigation, public security, life or limb or another or endangering the possible continued use of an undercover investigator. In cases involving the listening to and recording using technical means of the private speech of an accused on private premises as specified under section 100c(3) of the Code, notification is to be given within six months after the measure has been completed and any further deferral of notification requires the consent of a judge.

[5] A requirement for notification is imposed on States Members under principle 2(2) of the Council of Europe Recommendation on the use of data in the police sector which provides that "*Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.*" The United Kingdom has entered a reservation to this requirement on the ground that notification would diminish the value of interception.

affected might well jeopardise the long-term purpose that originally prompted the surveillance. Such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents.[6]

The revised recommendations

7.11 In Chapter 8 of this report, we propose that a supervisory authority should be created to keep the warrant and authorisation system under review. Having taken into account the considerations set out above, we do not recommend that there should be a mandatory requirement to notify the target in every case where a warrant or authorisation for surveillance has been granted. However, in those cases where the supervisory authority considers that a warrant or an authorisation has not been properly issued (or not issued at all), or the terms of a warrant or authorisation have not been properly complied with, the supervisory authority should be required to notify the person or persons subject to surveillance that there has been a contravention of the statutory requirements relating to the issue of the warrant or authorisation.

7.12 However, the supervisory authority should have the power to delay the notification if the authority is satisfied that notification would cause any prejudice to the purposes of the original intrusion.[7] The delay should be no longer than is necessary, but in exceptional circumstances of public security, such as those involving terrorism, there may be an argument that indefinite delay of notification to an aggrieved person is justified. In such cases, we recommend that the law enforcement agency concerned must seek an order from the court allowing notification to the aggrieved party to be indefinitely delayed. We contemplate that this would only be permissible in rare cases, however.[8]

7.13 The supervisory authority should keep the case under regular review and notify the persons concerned of the surveillance as soon as the reasons for the delay no longer apply. Where an individual approaches the supervisory authority for confirmation as to whether or not he has been the subject of surveillance, and surveillance has been carried out but cannot yet be revealed, the response from the supervisory authority should be "no

---

6 *Klass v Federal Republic of Germany* (1978) 2 EHRR 214, at para 58.

7 Where the target is likely to be the subject of surveillance in the future, notification is likely to make such surveillance more difficult. This approach would preclude the notification of recidivist offenders, or those where there was a reasonable prospect hat the investigation may be repeated in the future. Where the surveillance is made in respect of innocent parties, it would be prejudicial to notify innocent parties in particular cases if they could be expected to alert the target. Another possibility is that the law enforcement 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. In the particular circumstances of such cases, notification to the person or persons subject to the surveillance would be likely to cause actual prejudice to the purpose of the original intrusion. See consultation paper on *Privacy: Regulating Surveillance and the Interception of Communications*, at para 7.8.

8 One example might be where a terrorist organisation had been infiltrated by a law enforcement agency, but there has been a defect in the warrant.

comment". That could mean either that the person had not been under surveillance, or that he had been but the surveillance was legal, or that the surveillance was still ongoing.

7.14 If the notification process is to be effective, it is necessary that the supervisory authority is able to review an adequate number of warrants and authorisations. It would be impracticable to expect the supervisory authority to review every case, or to ask the law enforcement agencies to provide a report on every case to the supervisory authority. Instead, we recommend that the supervisory authority should be able to conduct random audits. In addition, we have recommended in Chapter 9 that the law enforcement agencies should submit quarterly reports to the supervisory authority, providing details, *inter alia*, of any errors discovered in the application for, and execution of, warrants and authorisations applied for.

7.15 We recognise that merely to inform an individual of the fact that he has been the subject of surveillance would be unhelpful. It would be necessary to notify the target of sufficient details of the surveillance as to enable him to decide whether or not he wished to seek compensation. The target should also be informed that, if appropriate, he has the right to apply to the supervisory authority for compensation.

Chapter 8

The supervisory authority

8.1 In this Chapter, we propose that a supervisory authority should be created to keep the warrant and authorisation system under review. The supervisory authority would review individual cases on its own motion in addition to receiving complaints or requests made by aggrieved persons.[1] We believe that the establishment of such a body would promote accountability and maintain public confidence in the regulatory system.

8.2 There are alternative models for such a supervisory authority, and a number of specific issues which need to be addressed in choosing the appropriate model:

- Composition of the authority – should this be a serving member of the Judiciary, or should the net be cast wider?

- Relationship between the authority and the courts – should the authority or the courts review the validity of authorisations for covert surveillance?

- Compensation – should the authority or the courts determine whether (and, if so, how much) compensation should be paid to an aggrieved person?

In considering these issues, and reviewing the sub-committee"s recommendations in the consultation paper, we have taken account of the statutory provisions relating to the interception of communications.[2] We have also taken into account the monitoring system in other jurisdictions, including the United Kingdom,[3] Australia,[4] and the United States.[5]

---

1 The lack of an "*independent or judicial oversight of decision-making to guard against possible abuse by the executive*" and the absence of any "*civil or criminal remedy for a breach*" of the Executive Order No 1 of 2005 were highlighted by Hartmann J in *Leung Kwok Hung v Chief Executive of the HKSAR* HCAL 107/2005 (judgment dated 9 February 2006).

2 A supervisory authority was not included in the *Interception of Communications Ordinance* (Cap 532), but the creation of such an authority (which would necessarily involve the expenditure of public funds) could not be included in a Private Member"s Bill, as this was. An aggrieved person could apply to the court for remedial relief under Part VII of the Ordinance. We have also taken into account the provision for regular reviews to be conducted by officers of a higher rank over the exercise of the powers to grant authorisation by designated authorising officers under the *Law Enforcement (Covert Surveillance Procedures) Order* (Executive Order No 1 of 2005).

3 Sections 65 and 67 of the *Regulation of Investigatory Powers Act 2000*. An Investigatory Powers Tribunal has been established under RIPA. The Tribunal is made up of members of the legal profession of at least 10 years" standing. One of the duties of the Tribunal is to consider and determine any complaints made to them by any aggrieved person over any conduct of surveillance which the person believes to have been carried out against him. The Tribunal must first investigate if any person has engaged in any such conduct and if so under what authority before it determines the complaint by applying the principles of judicial review.

The composition of the supervisory authority

Recommendations in the consultation paper

8.3 The sub-committee recommended in the consultation paper that a monitoring body should be established to carry out independent reviews of the authorisation of surveillance. The sub-committee recommended that a Justice of Appeal be appointed as the supervisory authority to review the issue of warrants authorising surveillance, applying the criteria for judicial review. The supervisory authority should be responsible for checking that the reasons given in the affidavits supporting the issue of the warrant were genuine and that the warrant had been complied with and executed in accordance with its conditions. The sub-committee considered and rejected a proposal that an existing body with an appropriate nexus and adequate administrative support could be used to take up the role of the supervisory authority.[6]

The Tribunal is not obliged to hear a complaint unless it is made within 12 months of the conduct to which it relates. The Tribunal may make such award of compensation or other order as it sees fit. The determinations, awards, orders and other decisions of the Tribunal shall not be subject to appeal or be liable to be questioned in any court. The Tribunal is under no duty to hold oral hearings but may do so where appropriate. Proceedings of the Tribunal shall be conducted in private. The complainant has the right to be legally represented. The Tribunal may receive evidence in any form, including hearsay evidence, but has no power to compel any person to give oral evidence. The Tribunal will merely inform the complainant of its determination but cannot report the reason for the decision. If it finds that no warrant or authorisation exists and that apparently no surveillance or interception is occurring, or that proper authorisation has been granted, it will merely inform the complainant that the complaint has not been upheld. The complainant will not know whether tapping had in fact occurred. However, if the complaint is upheld, the complainant will know that surveillance was occurring but unauthorised.

[4] Sections 54, 55, 57 and 61 of the *Surveillance Devices Act*. The *Surveillance Devices Act* 2004 empowers the Commonwealth Ombudsman (or his/her inspecting officers) to inspect the records of law enforcement agencies in order to determine whether statutory requirements have been met by the agency and its officers. The Ombudsman is given full and free access to relevant agency records, and may copy those records and require officers of the law enforcement agency concerned to provide relevant information. These inspections can be carried out during the currency of a warrant or authorisation but the Ombudsman can refrain from doing so at such time if he or she so chooses. At six-monthly intervals the Ombudsman must report to the Minister on the results of each inspection. The Minister must table the report in Parliament within 15 sitting days.

[5] Under the *Federal Wiretap Act* in the United States, a warrant to intercept communications may require reports to be made to the issuing judge showing what progress has been made toward achievement of the authorised objective. Such reports shall be made at such intervals as the judge may require. The requirement for regular progress reports helps to ensure that any possible abuses in the execution of the warrant are quickly discovered and halted. Section 2518(6) of the *Federal Wiretap Act*.

[6] The sub-committee considered whether an existing body such as the Privacy Commissioner or the Commissioner for Administrative Complaints could serve as the supervisory body. The sub-committee concluded that it would not be appropriate to involve the Privacy Commissioner in this distinct field of regulation as this would significantly affect his statutory role in ensuring fair play in data processing and the public perceptions of it: see consultation paper, at para 8.25. The option of utilising the Commissioner for Administrative Complaints was specifically rejected by the Commission in respect of interception of communications because of the Commissioner's restricted remit. The Commission noted that the Commissioner "*is excluded from investigating complaints relating to the Police or the Independent Commission Against Corruption, or matters affecting security, defence or international relations … in respect of*

8.4 The sub-committee also considered whether a separate complaints tribunal should be established, in addition to the supervisory authority. This was prompted by section 7 of the United Kingdom"s Interception of Communications Act 1985, which established an independent tribunal to investigate complaints regarding the issue of warrants. The sub-committee rejected this option on the basis, firstly, that it preferred the supervisory authority to undertake this function and, secondly, that aggrieved individuals would be able to pursue claims for compensation in the courts.[7]

Review of the recommendations in the consultation paper

8.5 We endorse the recommendation in the consultation paper that a new supervisory authority should be created to keep the proposed warrant and authorisation system under review. For the reasons identified by the sub-committee, we do not think it would be satisfactory to impose the functions we envisage for the supervisory authority on an existing body. We also agree with the sub-committee"s conclusion that there should not be a complaints tribunal separate from the supervisory authority, but that complaints relating to covert surveillance should be dealt with by the supervisory authority itself.

8.6 We do not agree with the proposal in the consultation paper, however, that a sitting Justice of Appeal should be appointed as the supervisory authority. We think that that would unnecessarily restrict the pool from which appointments could be made. We therefore recommend that the supervisory authority should be a serving or retired judge of the Court of First Instance, or a higher court, or a person eligible for appointment to the Court of First Instance. We recommend that the person appointed as the supervisory authority, should hold office for a period of three years and should be eligible for reappointment for a further period of three years. We further recommend that the supervisory authority be established with sufficient administrative support to properly carry out its functions.

The role of the supervisory authority

Recommendations in the consultation paper

8.7 The consultation paper recommended that the role of the supervisory authority should be to examine whether a warrant has been properly issued, and whether its terms have been properly complied with. It should be left to the supervisory authority to determine which warrants to examine, and on what basis. The supervisory authority should also receive

---

Hong Kong."" (LRC report on *Privacy: Regulating the Interception of Communicatio*ns, at para 8.39)

7 Consultation paper, at 8.42.

and examine complaints from persons who believe that they have been subject to covert surveillance by a law enforcement agency.[8]

8.8 The sub-committee took the view that the supervisory authority should be restricted to investigating whether a warrant had been properly issued, and should not pursue allegations of intrusions not sanctioned by a warrant:

> "*To initiate such an inquiry … , 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*."[9]

The sub-committee noted that the effective exclusion of the investigation of unauthorised surveillance from the supervisory authority"s remit coincided with the position in the United Kingdom. The sub-committee concluded that the supervisory authority should be restricted to investigating whether a warrant had been properly issued.

Review of the recommendations in the consultation paper

8.9 We endorse the sub-committee"s view that the principal role of the proposed supervisory authority is to serve as a monitoring body to keep under review the system of covert surveillance carried out by government departments or designated law enforcement agencies. The supervisory authority should be under a statutory duty to examine whether a warrant or internal authorisation has been properly issued, and whether the terms of a warrant or internal authorisation have been properly complied with or executed in accordance with its conditions.[10]

8.10 It would obviously be impracticable to expect the supervisory authority to review every instance of covert surveillance, or to ask the law enforcement agencies to provide a report on every case to the supervisory authority. Instead, we recommend that the supervisory authority should be required to conduct random sample audits of selected cases. This process

---

8 Consultation paper, paras 8.28 - 8.30.

9 Consultation paper, para 8.32.

10 A warrant may not have been properly issued, either because the statutory provisions had not been properly applied, or because the supporting affidavits contained inaccurate information.

would be facilitated by our recommendation in Chapter 9 that each law enforcement agency should submit a quarterly report to the supervisory authority, providing details, *inter alia*, of any errors discovered in the application for, and execution of, warrants and authorisations. Where the law enforcement agency discovers an error or irregularity, it should notify the supervisory authority of this at the earliest opportunity.

.

8.11 In addition, we recommend that where an aggrieved person believes he is, or has been, subjected to unlawful surveillance by a law enforcement agency he may request the supervisory authority to investigate whether there has been any contravention of the statutory requirements relating to the issue of that warrant or internal authorisation. The supervisory authority"s investigation should include circumstances where covert surveillance has been carried out without the issue of the requisite warrant or internal authorisation.

8.12 In its response to the consultation paper, the Bar Association proposed that an aggrieved party should have a right to apply to court to set a warrant aside.[11] The approach we favour, however, is that the supervisory authority should review the propriety of a warrant, rather than the court. As we explain at paragraph 8.19 below, we recommend that the supervisory authority should have the power to set aside a warrant where the authority finds that there has been material non-disclosure or misrepresentation in the application for the warrant. Restricting the review function to the supervisory authority reduces the risk that sensitive material may be unduly disseminated. We accordingly conclude that an aggrieved person should not have the right to apply to the court to set aside a warrant for covert surveillance.

8.13 To provide practical and effective redress to an aggrieved person, we recommend that the supervisory authority, in addition to its function of reviewing any impropriety in the issue or execution of a warrant or internal authorisation, should also be given the power to determine any award of compensation and to make such order as in its discretion it thinks fit, including orders for the destruction or retention of surveillance materials. We consider the issue of compensation in more detail later in this Chapter.

8.14 The supervisory authority should also be responsible for approving the internal guidelines on the granting of internal authorisations to be issued by each law enforcement agency, and the guidelines in respect of the retention, disclosure or destruction of materials obtained through covert surveillance or by covert means.

8.15 We recommend in Chapter 9 that the supervisory authority should be required to furnish an annual public report to the Legislative Council setting out information and statistics relating to the issue and execution of

---

[11] The grounds submitted by the Bar Association for setting aside a warrant are: (a) the warrant was wrongly issued, in the sense that the applicant"s evidence failed to establish the requisite criteria; (b) there was material non-disclosure or misleading evidence by the applicant in obtaining the warrant; or (c) the requirements of the warrant have not been properly complied with.

warrants and internal authorisations and to provide an overview on the operation and effectiveness of the regulatory system. The supervisory authority should further provide an annual confidential report to the Chief Executive containing details of individual cases.[12]

Review by the supervisory authority

The principles to be applied by the supervisory authority

8.16 The principles to be applied by the supervisory authority in reviewing the validity of a warrant or an internal authorisation should be those that are applied by a court on an application for judicial review.[13]

---

12 See paras 9.17 to 9.18 of Chapter 9.

13 In *Christie v United Kingdom* 78-A DR 119 (1994) (Application No 21482/93, judgment dated 27 June 1994), the applicant complained that his telexes from East European trade unions had been intercepted by the Government Communications Headquarters (GCHQ) which was the United Kingdom"s central intelligence-gathering centre. One of the grounds of the complaint was that the protection offered by the Tribunal set up under section 7 of the then *Interception of Communications Act 1985* to investigate complaints from any person who believed that communications sent by or to him had been intercepted was inadequate and ineffective. The European Commission of Human Rights held that the 1985 Act satisfied the requirement of Article 8 of the European Convention on Human Rights (which guarantees the right to privacy). As stated by the European Commission at 136 of the decision: "*The applicant criticises the limited nature of the examination of complaints carried out by the Tribunal, which has no power to consider the correctness of the Secretary of State's decision to issue a warrant, only whether the decision was one which no reasonable Secretary of State could have reached. … In the context of the 1985 Act, the Commission notes that the Tribunal is similarly constituted by lawyers of ten years' experience who act in an independent capacity. While it could not reconsider the merits of a decision to issue a warrant, it does have the competence, applying the judicial review standard, to investigate whether there has been a contravention of sections 2-5 of the 1985 Act, which would include reviewing whether the Secretary of State issued a warrant for a proper purpose. Further the Commissioner is under an obligation to review warrants under section 8(1)(a) of the 1985 Act. It appears from his 1987 report that in reviewing the issue of warrants he applies a vigorous test of whether they were <u>really</u> needed' for the purpose. … While the Tribunal and Commissioner have no express jurisdiction to investigate cases where no warrant has been issued, the Commission recalls that interceptions without a warrant are criminal offences and accordingly a matter for the police. If, however, the Tribunal or Commissioner came across an instance of an unauthorised interception, it is apparent from the Secretary of State's statement before Parliament that it would be expected that they would report it. In so far as the applicant complains that the Tribunals under the 1985 and 1989 Acts [Security Service Act 1989] are prevented from giving reasons which is not in the applicant's favour, this limitation has already been considered by the Commission in the context of the 1989 Act in the <u>Esbester</u> case where it found, on the basis of established case law, that States may legitimately fear that the efficacy of a system might be jeopardised by the provision of information to complainants and that the absence of such information cannot in itself warrant the conclusion that the interference was not <u>n</u>ecessary'… The applicant has also criticised the fact that the decisions of the Tribunals are not subject to any appeal to a court and casts doubts on their effectiveness, pointing out that neither Tribunal has ever made a determination in favour of a complainant. In addition, no parliamentarians play a role in the process, and, he submits, the effectiveness of the Commissioner must be in doubt since he has no independent source of information and cannot personally review every warrant. While the Commissioner does appear to choose warrants to review on the basis of random selection… the Commission is satisfied that his existence must in itself furnish a significant safeguard against abuse. The annual reports indicate that the Commissioner, a senior member of the judiciary, takes a thorough and critical approach to his function in identifying any abuse of the statutory powers. … The Commission notes that the possibility of review by a court or involvement of parliamentarians in supervision would furnish additional independent safeguards to the system. Having regard however to the wide margin of appreciation accorded to the Contracting Parties in this area, the Commission finds that the 1985 Act nonetheless satisfies the threshold requirements of Article 8 para 2 of the Convention in providing a*

8.17 The supervisory authority should determine whether the issuing authority has correctly applied the legal principles set out in the relevant legislation, and whether it has taken into account all relevant considerations and ignored factors that were irrelevant before making the decision to grant the warrant or internal authorisation.[14] The supervisory authority must be satisfied that the information or materials provided in the application to the issuing authority were sufficient to meet the conditions for the issue of a warrant or an internal authorisation such that the decision would not be regarded as manifestly unreasonable.

8.18 The supervisory authority should examine whether the proper procedures were followed in the application for, and the issue and execution of, the warrant or internal authorisation to ensure that there is no procedural irregularity in the authorisation process.

8.19 Where the supervisory authority finds that there has been material non-disclosure or misrepresentation of information in the application for a warrant or an internal authorisation, the supervisory authority should either set aside the warrant or internal authorisation if it is still effective, or declare that it has been improperly granted where the warrant or internal authorisation has expired.

Procedure for review by the supervisory authority

8.20 Because of the likely sensitivity of the materials and information relating to the application, issue or execution of a warrant or an internal authorisation, and the need to restrict their disclosure, statutory provision will have to be made to modify the normal rules of judicial process in certain specific respects. Firstly, because of their sensitivity, the supervisory authority should be under no obligation to grant full disclosure of all relevant

---

framework of safeguards against any arbitrary or unreasonable use of statutory powers in respect of an individual in the position of the applicant… .” Under the then 1985 Act, the role of reviewing the regulatory system for interception of communications on a random selection basis and of furnishing annual reports was carried out by a Commissioner appointed by the Prime Minister (pursuant to section 8 of the Act). The Tribunal set up under section 7 of the 1985 Act was solely responsible for investigating complaints from any person who believed that his communications had been intercepted unlawfully. Under RIPA *t*he Chief Surveillance Commissioner is under a duty to keep under review the performance of functions under Part III (authorisation of action in respect of property) of the Police Act 1997, and to make an annual report to the Prime Minister, a copy of which must be laid before both Houses of Parliament: section 107 of the Police Act. The Chief Surveillance Commissioner must keep under review, so far as they are not required to be kept under review by the Interception of Communications Commissioner or the Intelligence Services Commissioner, the exercise and performance of the powers and duties under RIPA: section 62(1) of RIPA. The Investigatory Powers Tribunal is the only appropriate tribunal that may consider and determine any complaints made to them by aggrieved persons: section 65(2) of RIPA. Although the supervisory authority proposed in this report is to carry out both the monitoring and the adjudication functions, we do not believe that there is a significant conflict of interest in the two roles, as the adjudicator would need to have full access to the information in order to adjudicate.

[14] See the recommendations on the grounds on which the Court of First Instance or an authorising officer of a designated law enforcement agency must be satisfied and the matters that are required to be taken into account for the issue of a warrant or an internal authorisation set out in Chapter 3 of this report.

materials to a complainant. Secondly, the supervisory authority should not be under any duty to give reasons for its decision. This is because the giving of reasons could in many cases disrupt the effectiveness of surveillance by revealing the fact of its existence.

8.21 Thirdly, in reviewing a warrant or internal authorisation for covert surveillance, the supervisory authority would not be required to hold any oral hearing. The person who has lodged a complaint or requested a review would not be entitled to make oral representations to the supervisory authority during the process of the review (unless invited to do so), but he would be entitled to make written representations at the time he submits his complaint or requests a review.[15] The review of the warrant or authorisation and the examination of any persons by the supervisory authority should be carried out in private. Counsel and solicitors should not have any right of audience before the supervisory authority but may appear before it if the authority thinks fit.

8.22 We recommend that the supervisory authority should be given the power to:

(a) summon before it any person who is able to give any information relating to the review and examine that person for the purposes of such review;

(b) administer an oath for the purposes of the examination under (a) above; and

(c) require any person to furnish to it any information (on oath if necessary) and to produce any document or thing which relates to the review.

8.23 The decision of the supervisory authority on the outcome of the review should not be subject to appeal or be liable to be questioned in any court.[16]

Matters to be considered in reviewing a complaint

8.24 In reviewing a complaint from an individual who believes that he is, or has been, subject to unlawful covert surveillance, the supervisory authority would need to ascertain whether any such intrusive conduct has been, or is still being, carried out by any government department or law enforcement agency. Where no covert surveillance has been carried out against the complainant by or on behalf of any government department or designated law enforcement agency, the supervisory authority should consider whether, on the information available, a criminal offence may have

[15] Though he would be entitled to be heard in any subsequent application for compensation: see para 8.36 below.

[16] The decision of the supervisory authority would, however, be subject to judicial review.

been committed by any private individual against the complainant, and if so, whether the matter should be referred to the relevant law enforcement agency for further investigation.

8.25 Where the supervisory authority finds that covert surveillance is being, or has been, carried out by a government department or a law enforcement agency, the supervisory authority must first ascertain whether a warrant or internal authorisation has ever been issued to authorise that surveillance in relation to the complainant. If the covert intrusion was authorised, the supervisory authority should examine whether the relevant statutory requirements for the issue or execution of the warrant or internal authorisation, as the case may be, were complied with. Where the covert surveillance is being, or has been, carried out by a government department or one of the law enforcement agencies without authorisation, the supervisory authority should ascertain whether authorisation, either in the form of a warrant or an internal authorisation, would be required under the circumstances of that particular case.

8.26 Where the supervisory authority concludes that there was a failure on the part of the relevant government department or law enforcement agency to obtain the requisite authorisation, or where the supervisory authority comes to the view that the warrant or internal authorisation for covert surveillance was not issued or executed properly, the supervisory authority should notify the complainant that there has been a breach of the relevant statutory requirements regulating covert surveillance and of his entitlement to apply to the supervisory authority for compensation. The supervisory authority may also make an appropriate order as set out at paragraph 8.31 below.[17]

Notification of the result of the review

Where there is a defect or irregularity in the issue or execution of a warrant or an internal authorisation

8.27 Where the supervisory authority determines that surveillance has been conducted but that a warrant or an internal authorisation has not been issued, or has not been properly issued or complied with, the supervisory authority should notify the person subject to surveillance and the relevant law enforcement agency that there has been a contravention of the statutory requirements relating to the issue of the warrant or internal authorisation.

8.28 As explained at paragraph 7.12 above, the supervisory authority should have power to delay notification to an aggrieved person if it is satisfied that notification would seriously hinder existing or future investigation of

[17] In reviewing the propriety of a warrant or internal authorisation, the supervisory authority should apply the principles applied by a court on an application for judicial review, and may consider whether the grant of the warrant or internal authorisation was unreasonable in juridical review terms. See para 8.16 above.

serious crime or prejudice the public security of Hong Kong. The delay should, however, be no longer than is necessary. The supervisory authority should keep the case under regular review and notify the aggrieved person of the result as soon as the reasons for the delay no longer apply.

Where no warrant or authorisation required or where the warrant or authorisation is in order

8.29 Where the supervisory authority concludes that:

(a) the complainant has not been subject to covert surveillance which requires the issue of a warrant or internal authorisation; or

(b) a warrant or authorisation has been properly issued or complied with,

the supervisory authority should refrain from making any comments other than informing the complainant that there has not been any contravention of the statutory requirements relating to the issue of warrants or internal authorisations.

8.30 We consider it inappropriate to notify the complainant that the surveillance was conducted in accordance with a properly issued warrant or internal authorisation because this would run the risk of rendering any ongoing investigation futile as the suspect may have connections with the aggrieved person, or he may be the aggrieved person himself. Neither should the complainant be notified that there is no warrant or authorisation in existence since this would provide a suspect with a backdoor way of verifying whether he has or has not been a target of covert surveillance by a law enforcement agency.

Orders by the supervisory authority on completion of review

Where the warrant or internal authorisation remains in force

(a) Statutory requirements breached

8.31 If the supervisory authority concludes that any officer of a government department or law enforcement agency has, in the purported exercise of their official duties, contravened any statutory requirements in relation to the issue or execution of a warrant or internal authorisation which is still effective, the supervisory authority must:

(a) set the warrant or internal authorisation aside; and

(b) make such order as the supervisory authority in its discretion thinks fit, including:

(i) the destruction of the surveillance materials; or

(ii) the retention of the surveillance materials where they are required to be used as evidence to establish the illegality of the surveillance or to be used in subsequent civil or criminal proceedings.

(b) Statutory requirements complied with

8.32 Where the supervisory authority is satisfied that the warrant or internal authorisation has been properly issued and complied with, it may still in its discretion make any of the orders specified in paragraph 8.31(b) above in relation to the disposal of the surveillance materials obtained under the warrant or authorisation.

Where the warrant or internal authorisation has expired

8.33 Where the warrant or internal authorisation in question has expired, there is no warrant or internal authorisation to be set aside. The supervisory authority would still have the power to make such order as it thinks fit in respect of the destruction or retention of the surveillance materials as set out in paragraph 8.31(b) above.

Compensation

8.34 We consider that an aggrieved person should be entitled to compensation for intrusion into his privacy as a result of unlawful covert surveillance by a government department or law enforcement agency. There are practical difficulties, however, as the sensitivity of covert surveillance renders it difficult, if not impossible, for an aggrieved person to secure sufficient evidence to bring a civil claim for compensation for unlawful covert surveillance, or to establish the seriousness of the intrusion into his privacy.

8.35 In balancing the need to protect the privacy of the individual and the public interest in maintaining the secrecy of the surveillance capabilities of the law enforcement agencies, we consider that the most feasible option would be to allow an aggrieved person to seek compensation for unlawful intrusion into his privacy through an application to the supervisory authority. In doing so, we endorse the views we have expressed in the report on *Privacy: Regulating the Interception of Communications*:

> *—Given that both the warrant application and the interception were carried out by the authorities in secret, the aggrieved person would have difficulty in seeking legal remedy if he suffers any loss by reason of a breach of the statutory requirements. In order to protect the secrecy of interception activities carried out by the law enforcement agencies, the aggrieved person would simply be notified of the existence of a breach; he would not be*

informed of the reasons for coming to that conclusion. He would therefore have an impossible task in securing enough evidence to prove that there had been an unlawful interception and that he had been the object of that interception. Due to the sensitivity of the matter, the authorities would also be reluctant to disclose the details of the application and other relevant confidential material in open court. It is therefore impractical to ask the aggrieved person to seek compensation by taking civil proceedings.

In order to provide a practical and effective remedy for the aggrieved person, the supervisory authority should have power to award compensation to the aggrieved person if the authority concludes that the warrant has been improperly issued or complied with, or if the warrant has been set aside… .That compensation would be paid out of public funds. We think it right that before reaching any conclusion on the question of compensation, the supervisory authority should give the aggrieved person an opportunity to be heard on this issue. …

We believe that any loss suffered by the aggrieved person, including any injury to his feelings, would be adequately compensated by such compensation as may be awarded by the supervisory authority. To avoid re-opening issues in court proceedings, the aggrieved person should not be allowed to claim damages in court if he has already been awarded compensation by the authority. This is not to deny the right of an aggrieved person to seek legal remedies. On the contrary, our proposal takes account of the practical difficulties of an individual in claiming damages by bringing a legal action of his own. We believe that compensation awarded by the supervisory authority would provide a far more practical and effective redress to the aggrieved person without at the same time compromising the secrecy and effectiveness of the interception activities."[18]

8.36 We do not consider it essential to provide an aggrieved person with access to materials relating to the application, issue or execution of the warrant or internal authorisation for covert surveillance in an application for compensation.[19] However, in principle we believe that this evidence should

---

18 Report on *Privacy: Regulating the Interception of Communications,* Hong Kong Law Reform Commission, paras 8.77 to 8.79.

19 In *P.G. and J.H. v The United Kingdom* (Application No 44787/98), it was held by the European Court of Human Rights, at paras 68 - 71, that the entitlement to disclosure of relevant evidence (which involved an expert report relating to the secret surveillance measures in that case) is not an absolute right even in criminal proceedings: "*In any criminal proceedings there may be competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of criminal investigation, which must be weighed against the rights of the accused… In this case, the prosecution did not disclose to the defence part of a report… relating to the surveillance measures and instead submitted it to the judge. When [the expert witness] gave evidence and refused to answer certain questions put in cross-examination by defence counsel which related to the background to the surveillance, the judge*

be provided unless there is a public interest justification for not doing so. We recognise that that may still severely limit the evidence, but it should not automatically exclude it all. We agree that before reaching any decision on the award of compensation and on the making of any order for disposal of surveillance materials, the supervisory authority should give the aggrieved person an opportunity to be heard on the issue.

8.37 We further recommend that the supervisory authority may include in its award of compensation such amount as it considers appropriate for injury to feelings, and may, where appropriate, award punitive damages.

8.38 We consider that where a court convicts a person of one of the criminal offences proposed in Chapter 1 of this report, an aggrieved person should be entitled to apply for damages to be paid to him by the defendant.

---

put those questions to the witness in chambers and took the decision, weighing the harm to public interests against the slight benefit to the defence, that part of the report and the oral answers should not be disclosed. The Court [European Court of Human Rights] is satisfied… that the defence were kept informed and were permitted to make submissions and participate in the above decision-making process as far as was possible without revealing to them the material which the prosecution sought to keep secret on public interests grounds…. The fact that the need for disclosure was at all times under assessment by the trial judge provided a further, important safeguard in that it was his duty to monitor throughout the trial the fairness or otherwise of the evidence being withheld…." It was held by the European Court that the non-disclosure of the surveillance material did not violate the right to a fair hearing in that case.

Chapter 9

Reports

The need for reports

Recommendations in the consultation paper

9.1 The consultation paper recommended that the supervisory authority should furnish annually a confidential report to the then Governor and a public report to the Legislative Council. The consultation paper recommended that there should be a statutory requirement that the reports should include the following information:

- the number of warrants issued
- their average length and their extensions
- the classes of location of the surveillance (ie domestic, business, etc)
- the type of surveillance device used
- the number of persons arrested and convicted as a result of the surveillance or intercepts.[1]

Review of the previous recommendations

9.2 Those responding to the consultation paper all supported the need for a reporting requirement, although there were different views on the types of information that should be included in the report.

9.3 We note that under the *Interception of Communications Ordinance* (Cap 532), the Legislative Council may at any time require the Secretary for Security to provide information on matters relating to the issue and execution of warrants for interception of communications for any specified period.[2] We also note that periodic reports are required to be published providing statistics and other information relating to the interception of communications and surveillance activities in the United States,[3] Canada[4], Australia,[5] and the United Kingdom.[6]

---

1 Para 8.34, consultation paper.

2 Section 11, *Interception of Communications Ordinance (Cap 532)*.

3 Section 2519*,* US *Wiretap Act.* Annual reports must be made to different bodies at different levels, providing information on the incidence, costs and effectiveness of interceptions

9.4 We believe that detailed annual reports play a crucial role in increasing public accountability for, and in enhancing transparency of, intrusive activities carried out by the law enforcement agencies. Taking these considerations into account, we agree with the recommendation in the consultation paper that the supervisory authority should furnish annually a public report to the Legislative Council and a confidential report to the Chief Executive. The system we envisage would therefore involve three reports: (i) a quarterly report from each government department and law enforcement agency to the supervisory authority to enable the authority to track particular cases where warrants or internal authorisations have been issued; (ii) an annual public report to the Legislative Council; and (iii) an annual confidential report to the Chief Executive.

The report to the Legislative Council

9.5 We recommend that the information that must be included in the report to the Legislative Council should be specified in the legislation. On reviewing the relevant recommendations in the consultation paper, we have made some revisions to the categories of information which we propose should be included in the report.

---

engaged in for law enforcement purposes in the United States. Within 30 days of the expiration of an order authorising interception (or each extension thereof) or the denial of an order, the issuing or denying judge has to report to the Administrative Office of the United States Courts providing particulars of the interception. The prosecuting authority has to make an annual report to the same Administrative Office. In April of each year the Administrative Office has to transmit to the Congress an annual report concerning the number of applications for orders authorising or approving the interception of wire, oral, or electronic communications and the number of orders and extensions granted or denied during the preceding year. The report must include a summary and analysis of the data required to be filed with the Administrative Office.

[4] Section 195, Part VI, *Criminal Code* of Canada. The Criminal Code requires yearly reports to be prepared by the Solicitor General of Canada setting out information on authorisations for interception of private communications and a general assessment of the importance of interception of communications for the investigation, detection, prevention and prosecution of offences in Canada. A copy of the report is to be laid before Parliament.

[5] Sections 49 and 50, *Surveillance Devices Act 2004* of Australia. A law enforcement agency must report to the Minister providing information as to whether the warrant obtained was executed, who executed the warrant, the kind of device used, the period of use, details of where the device was installed, how the use of the device benefited the investigation of a relevant offence and how the conditions of the warrant were complied with. Any extensions or variations of the warrant must also be stated. The Minister must table the report in Parliament within 15 sitting days of receiving it.

[6] Section 107, *Police Act 1997*. *T*he Chief Surveillance Commissioner is required to make an annual report to the Prime Minister on the discharge of his functions relating to the grant and execution of authorisations and appeals in respect of any interference with property. The report must be presented to Parliament and published as a Command Paper. The Prime Minister may exclude matters from the report if it appears to him that it contains matter "*prejudicial to the prevention and detection of serious crime*" or to the discharge of the functions of a police authority and relevant law enforcement agencies.

Information relating to warrants and authorisations

9.6 The report should state the number of warrants and authorisations for covert surveillance applied for, withdrawn, rejected, granted as requested and granted subject to modifications. The report should provide this information separately in respect of each of the law enforcement agencies. The average length of the warrants and authorisations granted, and of any renewals, should also be reported.

9.7 The number of warrants and authorisations which the supervisory authority has found on review were not properly issued or executed should also be specified in the report. The report should also include information on the destruction of materials gathered through covert surveillance.

Information on classes of location of the surveillance

9.8 We endorse the recommendation in the consultation paper that the "*classes of location of the surveillance*" should be stated. It would be sufficient to mention a general class of location at which covert surveillance was conducted, such as whether the surveillance was targeted at residential or commercial premises.

Information on class of devices used

9.9 Instead of stating the "*type of surveillance device used*", we recommend that the "*class of devices used*" (for instance, visual, oral or location tracking devices) to conduct the covert surveillance should be specified.

Information on categories of crimes involved

9.10 The major categories of crimes (including "serious crimes"[7]) in respect of which surveillance was conducted should be stated in the report.

Information on number of arrests and prosecutions as a result of surveillance

9.11 The consultation paper recommended that "*the number of persons arrested and convicted as a result of the surveillance*" should be specified in the report. One respondent to the consultation paper commented that it would be difficult to identify any accurate correlation because of the gap in time between the gathering of intelligence, the arrest, and the subsequent prosecution and conviction.

---

[7] As defined in Chapter 3 of this report.

9.12 We accept that it would be difficult for the law enforcement agencies to establish how many convictions were a direct consequence of the fruits of surveillance. We have therefore decided to revise the recommendation so that the report would only need to present statistics relating to the effectiveness of covert surveillance in leading to arrests and prosecution. Reference to "prosecutions" instead of "convictions" would in our view more accurately reflect the effectiveness of the surveillance, since a failure to convict does not necessarily mean that the surveillance was unwarranted or ineffective.

Information on the number of reviews and the findings

9.13 We recommend that the total number of reviews undertaken by the supervisory authority (including the number of referrals to the Court of First Instance) and the number of reviews carried out in response to a request by an aggrieved person should be set out in the annual report. The supervisory authority should also provide an overview of the findings and conclusions of the review in respect of the application of the warrant and the authorisation system.[8]

The confidential report to the Chief Executive

9.14 The material contained in the annual report to the Legislative Council will consist of aggregate statistics and information. It would clearly be inappropriate to include in a public report details of individual cases. To do so would breach the privacy of the individual concerned, and might compromise the effectiveness of any surveillance carried out by the law enforcement agency concerned. We believe that such information should, however, be contained in the confidential report made annually to the Chief Executive as a means of ensuring proper oversight. We envisage, for instance, that where the law enforcement agency used a device for surveillance in a particular case where they should have applied for a warrant, details of that case should appear in the report to the Chief Executive, but the report to the Legislative Council would state only that there had been a certain number of cases in which such irregularity had occurred.

9.15 We therefore endorse the recommendation in the consultation paper that the supervisory authority should furnish annually a confidential report to the Chief Executive. The report should cover such matters as are considered relevant by the supervisory authority, or such other matters as are required by the Chief Executive.

---

[8] The Hong Kong Journalists Association in its submission on the consultation paper proposed that the public report should include a section on "*warrants issued to monitor communications by media outlets*". We take the view that media and non-media should be treated alike. As the warrant procedure is to be under the control of judges and the issue of warrants and authorisations for surveillance are subject to review by an independent supervisory authority, such a system should secure public confidence.

Reports by government departments and law enforcement agencies

9.16 In order to assist the supervisory authority in carrying out its functions, any law enforcement agency or government department which has applied for a warrant or which has issued internal authorisations for covert surveillance should be required to furnish quarterly reports to the supervisory authority. Each agency or department"s quarterly report should provide the following information:

(a) the number of warrants and authorisations applied for, withdrawn, rejected, granted as requested and granted subject to modifications during the reporting period;

(b) the number of renewals sought and denied;

(c) the nature and location of covert surveillance carried out by its officers under a warrant or authorisation;

(d) the average duration of each surveillance carried out under a warrant or authorisation which has expired within the reporting period;

(e) the offences for which surveillance has been used as an investigatory method;

(f) the number of persons arrested and prosecuted as a result of the covert surveillance;

(g) any errors discovered by a law enforcement agency in the application for, and the execution of, a warrant or authorisation; and

(h) information on the destruction of materials gathered through surveillance.

The revised recommendations

9.17 The supervisory authority should furnish annually a public report to the Legislative Council. There should be a statutory requirement that the following information in respect of each government department and law enforcement agency be included in the report to be furnished by the supervisory authority:

(a) the number of warrants and authorisations for covert surveillance applied for, withdrawn, granted as requested and granted subject to modifications;

(b) the average length of warrants and authorisations granted and of any renewals;

(c) the number of warrants and authorisations which the supervisory authority has found on review were not properly issued or executed;

(d) the number of instances reported by law enforcement agencies to the supervisory authority, or discovered by the authority on review, where covert surveillance was carried out without the requisite warrant or internal authorisation having been issued;

(e) information on the destruction of materials gathered through covert surveillance;

(f) the class of location at which covert surveillance was conducted (for example, whether the surveillance was targeted at residential or commercial premises);

(g) the class of device used (for instance, visual, oral or location tracking device);

(h) the major categories of crimes (including "serious crimes") involved;

(i) statistics relating to the effectiveness of covert surveillance in leading to the arrest and prosecution of those charged with crime;

(j) the total number of reviews undertaken by the supervisory authority and the number of reviews carried out in response to requests by aggrieved persons; and

(k) an overview of the findings and conclusions of the review conducted by the supervisory authority in respect of the application of the warrant and authorisation system.

9.18 The supervisory authority should furnish annually a confidential report to the Chief Executive. The report should cover such matters as are considered relevant by the supervisory authority or as are required by the Chief Executive.

9.19 Each law enforcement agency or government department which has applied for a warrant or which has issued an internal authorisation to undertake covert surveillance should be required to furnish quarterly reports to the supervisory authority. The quarterly reports should provide the information specified in paragraph 9.16 above.