立法會 CB(2)2856/05-06(01)號文件
LC Paper No. CB(2)2856/05-06(01)

INTERCEPTION

OF

COMMUNICATIONS

AND

SURVEILLANCE BILL

Submissions from

M Jackson, Associate Professor,
and J Brabyn, Lecturer

Faculty of Law,
University of Hong Kong.

CONTENTS

THE INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE BILL

SUMMARY OF SUBMISSIONS

SUBMISSION 1:
The definition of 'covert surveillance' should be as wide and comprehensive as possible consistent with the boundaries of the concept and, in particular, should include all covert surveillance activity we would wish to be subject to at least reporting and monitoring by our agents outside the LEA community.

SUBMISSION 2:
'Covert surveillance' should not be restricted to surveillance using surveillance devices.

SUBMISSION 3:
'Covert surveillance' should not include observation or eavesdropping in public places unassisted by surveillance devices arising other than in pursuance of a pre planned targeting of an individual, group of individuals or place.

[Pre-planned means planned before the person observing or eavesdropping identified the intended target.]

SUBMISSION 4:
The term 'systematic' should be omitted from the definition of 'covert surveillance'.

SUBMISSION 5:
The proposed para (b) should not be added to the definition of 'covert surveillance. Rather section 5(2) should be amended to read:

*(2) Subsection (1) does not apply to any covert surveillance carried out pursuant to a prescribed authorization or to any covert surveillance carried out as a necessary spontaneous reaction to unforeseen events or circumstances for which subsequent authorization was obtained pursuant to s. *.*

The reference to section * reflects the consequential need for a separate section * specifically dealing with spontaneous surveillance and the need for subsequent reporting and authorization.

SUBMISSION 6:
Only **necessary** spontaneous surveillance should be exempt from prior authorization.

SUBMISSION 7:
Surveillance of premises, places and organizations should also require authorization and be subject to monitoring etc.

SUBMISSION 8:
If the substance of the present section 2(2) is retained, it must at least be made clear that 'activity' does not include having conversation in a normal tone with specific persons.

SUBMISSION 9:
The definition of public place should in any case be reconsidered and included in the Ordinance in full, without reference to other legislation, certainly not to the inappropriate provision in the Summary Offences Ordinance.

SUBMISSION 10:
Remembering that permission to engage in such surveillance can be obtained by phone and that spontaneous following of suspects detected at the scene or unexpectedly is permissible, a decision to follow/ stake out a person or place should be treated as covert surveillance Type 2 even when that person enters a public place, including a public vehicle.

SUBMISSION 11:
The phrase 'likely or intended' would be a better formulation.

SUBMISSION 12:
Legitimate purposes for which interception or covert surveillance might be carried out should **explicitly** include 'obtaining evidence for proving the commission of a serious crime in a court' and fulfillment of the HKSAR's mutual assistance obligations.

SUBMISSION 13:
Specific references to 'residents' or 'other persons within Hong Kong' should not be included in any definition of "public security".

SUBMISSION 14:
The offences relating to unauthorized and unlawful assemblies in the Public Order Ordinance should be expressly excluded from the definition of "serious crime" for the purposes of Type 2 surveillance.

SUBMISSION 15:
The whole structure of clause 3 should be revised – and simplified.

The term 'balancing' should be avoided.

The authorizing provision should in terms state that authority for interception/ covert surveillance **will not be granted unless** the judge/ authorizing officer, having carefully considered the specific aspects of the privacy right being challenged (not merely but including the degree of intrusiveness) and the specific circumstances of the applicant's case (not merely but including the factors set out in clause 3 as it now appears) is satisfied that the government has established the need for and proportionality of the specific limitation requested.

SUBMISSION 16:
Even if, contrary to the above, the present structure is retained, the phrase 'in operational terms' should be omitted.

SUBMISSION 17:
The panel judge/ authorizing authority/ should be specifically required to consider the quality (reliability and sufficiency) of the evidence upon which the law enforcement agency relies in selecting the surveillance target and advocating the need for surveillance.

SUBMISSION 18:
Breach of the prohibitions in sections 4 and 5 should provide a sufficient basis for an action in court – with appropriate remedies available such as the destruction of information, apologies and compensation.

SUBMISSION 19:
Applicants for authorization should be required to show that they have reasonable grounds for their honest belief that the proposed surveillance of this particular target is necessary and proportional in pursuit of one of the legitimate objectives.

SUBMISSION 20:
Surveillance product obtained by interceptions or surveillance conducted pursuant to [spontaneous], emergency or oral authorizations where no subsequent authorization was obtained within the requisite time period should not be destroyed until so ordered by either (i) a panel judge or authorizing officer (where application was made but rejected) or (ii) by the Commissioner (where no application was made).

Such surveillance product should be sealed and not available for use by any LEA unless otherwise authorized by the Commissioner.

SUBMISSION 21:
The Commissioner's monitoring functions should extend to actively monitoring the decisions of the Panel Judges.

SUBMISSION 22:
The Commissioner should be selected from past/ present judiciary above the rank of the Panel Judges. i.e. at least at appellate level.

SUBMISSION 23:
When an application for an examination has been received, the Commissioner must have the responsibility and all the necessary investigatory powers to determine the questions of fact raised by the examination.

SUBMISSION 24:
The Commissioner's determination as to whether upon the established facts a communication transmitted to or by a person seeking an examination has been intercepted or such person has been subject to covert surveillance otherwise that pursuant to a RELEVANT, VALID AND CURRENT PRESCRIBED AUTHORISATION should not be hampered or complicated by the complex rules and sometimes artificial limitations of judicial review.

SUBMISSION 25:
The powers under clause 51 should expressly extend to the fact finding stage of the examination process.

The Commissioner's orders under this section should be in the nature of a judicial warrant and should be enforceable in the same way as a warrant.

Failure to produce a requested report should be a serious disciplinary offence, arguably a criminal offence analogous to a contempt.

Failure to produce a requested report should require the Commissioner to conclude appropriate issues of fact against the relevant LEA, for example, that the relevant procedures were observed, that the relevant officers acted in good faith etc.

SUBMISSION 26:
The Commissioner should have an express power to recommend disciplinary action against specific individuals to their respective Heads of Department or, if a Head of Department is a target of the SUBMISSION, to the Chief Executive.

SUBMISSION 27:
There should not be any absolute bar on the use of the product of an interception in a criminal trial.

The government should always have a discretion to release product for use in a criminal trial to the prosecution and/ or the defence – just as they may decide to use evidence of an informant or not.

The prosecution must disclose the existence of any product that may assist the defence to the trial judge.

A trial judge should have the power to order disclosure to the judge as contemplated in the Bill, except that the requirement of satisfaction that disclosure is 'essential in the interests of justice' before the judge has even seen the product is too high a test.

The prosecution must have the right to abandon the prosecution rather than disclose the product as ordered by the judge.

The trial judge may review the content of disclosed product and order the prosecution to stipulate to certain facts in the manner currently envisaged.

PRELIMINARY OBSERVATIONS – THE GUIDING PRINCIPLES

We have approached the Bill with the following guiding principles in mind :

(a) The value of privacy

Private space away from the prying eyes and inhibiting influence of government, private institutions, even neighbours, is essential for the individual and collective intellectual, cultural and emotional growth and well being of humans.

Private space is also an important safeguard of our freedom, of our ability to keep governments and other power wielders at a manageable and bearable distance.

Knowledge about people (their movements, associates, thoughts, preferences, activities, finances, politics etc) facilitates exercise of physical, financial, political, social, intellectual and emotional power and influence over those people. The more governments/ employers/ corporations/ individuals know about us, individually and collectively, the easier it is for them to exert power and influence over us. Therefore it is important that no one entity knows too much – and that those who do know are not able or permitted to misuse their knowledge.

(b) The need for protection of privacy

We cannot rely upon the restraint of others in their acquisition and use of knowledge about us to protect our freedom. We need to be able to control what is known of us by others and, where that is not possible, at least to control what use others can make of the information they know. We need to be able to protect our privacy.

A hundred and fifty years ago, at least in the absence of spies, informers and corrupt servants or employees, protecting our privacy was a relatively simple matter. The four walls of our dwellings, the openness of our means of transportation, the absence of written records for most of our cash/ barter transactions, the impracticality of collecting and collating such

records as there were, bank secrecy practices and the severe limits of technology protected us to a substantial degree. Consequently, while the common law developed the tort of trespass which at least incidentally protected the privacy of our real property and legislation protected the Royal Mail and telephone communications, neither common law nor parliament developed a general right of privacy, protected by tort or the criminal law.

In the modern world of computers, telecommunications and rapidly evolving technology, protecting our privacy has become extremely difficult. In the absence of legal impediments – and assisted by significant (unwary) public indifference – modern governments and private institutions have used our ever advancing technology to develop processes for gathering, collating, storing, sharing information about people that reach almost every aspect of our lives.

Maintaining even minimal privacy for individuals and collectivities now requires vigorous pro-active privacy protection.

A strong right of privacy that is effective viz-a-viz government/ private institutions and neighbourly intrusions on our privacy – particularly in the form of information gathering, collating, storing, dissemination and use – has thus become essential.

(c) The need for surveillance

Even in HK, the efficient and effective detection, prevention and prosecution of serious crime, both within the HKSAR and elsewhere, and also the protection of the territorial and economic security of HK, the PRC and other jurisdictions, can be assisted by and may even require HKSAR law enforcement personnel to use highly invasive interception of communication and/ or covert surveillance techniques to gather information and evidence.

It is good to be able to detain and incapacitate the perpetrators of serious crimes. It is much better to be forewarned of the criminals' plans and to be able to thwart them. Forewarning requires intelligence and intelligence requires informants, vigilant and intelligent surveillance – and luck.

(d) The danger of official covert surveillance

Even the existence of the possibility of using surveillance of any kind to gather information about people and organizations threatens and practically limits individual and social privacy. Actual use of surveillance is the antithesis of privacy.

Therefore the danger of official surveillance is the threat it represents to our essential privacy. Proactive protection of our privacy requires proactive limitation of official surveillance so that the threat and damage to our privacy is restricted to acceptable levels.

Surveillance we know about is relatively easy to control. However, where the surveillance is covert, there are enormous problems. It is in the nature of covert surveillance that those who are being surveyed must not know it – they must be watched, listened to, recorded, photographed unawares. Covert surveillance must be secret.

It is that secrecy that gives rise to the special danger of covert surveillance for the freedom of a people. The need for secrecy makes our effective control of covert surveillance, even ex post facto monitoring and accountability extremely difficult. But it doesn't remove the necessity for such control and accountability. Quite the contrary. Without effective control and accountability what the agencies were doing in terms of surveillance would not be known – or even knowable – by anyone outside the agency loop. The agencies involved would become a power and a law unto themselves – and that is always a dangerous thing. In the absence of effective control and accountability, it is inevitable that, even with all relevant personnel acting in good faith, use of surveillance would become excessive, it would sometimes be used for improper purposes, there would be misuse of information obtained by surveillance and so forth. It would even be possible for those in positions of power to co-op the agencies and obtain the use of their surveillance powers for their own ends – and we might never know.

(e) How to keep covert surveillance within acceptable bounds

Articles 30, 29 and 39 of the HKSAR Basic Law, the latter read in conjunction with the ICCPR and the Bill of Rights, require the privacy of communications of HK residents and of their homes in particular, perhaps

their privacy in general, to be (i) protected against government interference by law and (ii) subject only to inspections or other intrusions by government 'in accordance with legal procedures' or 'prescribed by law'.

There are currently no sufficient legal procedures under which non consensual interception of private communications/surveillance by the government can be authorized by law as required by the Basic Law.

Leung Kwok Hung and Another v *Chief Executive of HKSAR*
HCAL 107/2005

A law that restricts where necessary and otherwise regulates the widest possible range of interception/ covert surveillance by government personnel is a basic minimum for securing control of and accountability for such surveillance.

Impractical laws invite disrespect and circumvention. A law that respects the legitimate needs of law enforcement can more effectively demand to be respected by law enforcement in return. Therefore, the law must be practical in the sense that it enables law enforcement agencies acting in good faith to do everything they reasonably need to be able to do to achieve their legitimate objectives **legally, without fear of civil law or criminal repercussions and without unnecessarily impeding red tape.** Government personnel acting in good faith for the protection of public safety should not need to be prepared to break the law – or even Codes of Procedures – in order to do what is necessary and proportional in order to properly do their jobs.

Nevertheless, it is for society and not the government, let alone law enforcement, to determine in general/ principle, what is necessary and proportional and what is intolerable intrusion or violation. That determination should be made clear in the terms of the law. The law must clearly identify the limits of legitimate surveillance and effectively prohibit all illegitimate surveillance. The formal legislation should be supplemented by binding Codes of Practice that clearly spell out the detail.

It is a strength of our present system that the CE and Secretary for Security do not interfere in the day to day running of our law enforcement agency.

To the outsider at least, there appears to be a reasonably healthy balance between high level policy control, accountability and independence.

Such a balance is crucial in the context of surveillance. The CE or Secretary for Security must be able to request surveillance assistance/ priority for legitimate purposes (legitimate direction/ use) and to insist upon receiving regular reports about surveillance activities and even to demand explanations of specific surveillance activity (accountability). The law enforcement agencies must have obligations of disclosure and reporting (accountability) and co-operation (legitimate direction/ use) but must also be able to resist any attempt by government to co-op/ restrict their surveillance activities for illegitimate ends or to interfere in the operational decisions necessary for a specific activity (independence). In the latter situation, law enforcement must be able to stand on the terms of the law.

The silence of covert surveillance must be broken. Somehow, everything that is planned and executed, that is, all and any surveillance activity planned or carried out by HK law enforcement agency or government official of any kind must be known by – or at least open to inspection and examination and capable of being known by – independent persons of ability and stature who are otherwise outside the government or surveillance loops, true independents who will be able to effectively observe and moderate implementation/ non implementation of the relevant law. (control and accountability)

The law must provide a mandatory system of (i) prior authorization procedures and (ii) rigorous ex post facto reporting, monitoring and examination obligations and powers, such prior authorization and ex post facto scrutiny to be the responsibility of persons OUT SIDE the law enforcement/ executive loop.

The public cannot know of covert surveillance directly but their representatives must know – everything. There must be at least one person, preferably more than one person so as to make corruption more difficult, whose responsibility is to know, to find out and not merely to accept what that person has been told.

That person(s) will report to the CE – and, as much as possible, to the public so that the power of informed public opinion will replace the shield of secrecy.

In this way, the watched will be able to keep a close watch and check on the watchers without preventing the watchers from doing their job.

(f) A culture of respect for law and privacy, not a culture of secrecy

Maintenance of the rule of law in a society requires a commitment to the observance of laws by the vast majority of the community – and most especially by the government (and all its agencies), the legislature and the judiciary. Our criminal prohibitions are workable only because and in so far as they are believed in and hence observed by most of us. Punishment for breach of these prohibitions is our last line of defence, not our first.

The same is true of the protection of human rights. We need laws declaring and protecting those rights, and those laws must have enforcement teeth – but our right of privacy depends mostly upon our belief and support, and the belief and support of our law enforcement officers, judges, law makers and government. We all have to believe privacy is important and act accordingly for our right of privacy to be protected.

For law enforcement agencies, a commitment to privacy as an important value worthy of and entitled to protection may require regular if not constant reinforcement but no law or legal regime has any hope of consistent success without such a commitment.

(g) On matters of evidence

Prior to the recent institutionalization of human rights and putting to one side evidence of confessions allegedly made to persons in authority by criminal defendants, the common law did not prohibit the prosecution from adducing – or give the judiciary a general discretion to exclude – unlawfully obtained evidence by reason of that illegality alone. The position might have been different if reliability of the evidence was also affected. Contra positions, such as those that evolved in the USA under a

constitutional guarantee of due process and in the face of significant and widespread excesses, were thought to sacrifice the interests of actual or potential victims of crime to admittedly substantial general public interest in maintenance of due process in an inappropriate way. The process of controlling and disciplining law enforcement personnel was said to be better dealt with in a different way, by resort to the general laws of tort and crime or by internal disciplinary procedures.

Unfortunately, neither tort nor criminal law provided real protection and there is strong evidence that unlawful search and seizure/ surveillance were not controlled by disciplinary procedures. The availability of other means of controlling the police etc. was a convenient myth.

If the common law's approach to the admissibility of unlawfully obtained evidence is to be maintained, even in the face of proven violations of Basic Law guarantees of protection of privacy, effective protection of our right of privacy requires that the myth become a reality.

Law enforcement personnel, backed by panel judges and an independent commissioner as proposed, must take up the essential function of ensuring good faith compliance with both the law and best practice codes and pursue that function rigorously.

The present theoretical possibility that unlawful searches, seizures – even trespasses or assaults – might give rise to an action in tort or criminal prosecution for assault or criminal damage against the relevant law enforcement personnel/ agency must become a reality. Disciplinary consequences for mala fides breaches of procedure – perhaps even grossly negligent breaches – must become the norm. If privacy is to stand any chance against modern technology, law enforcement agencies must develop a privacy protection culture.

There is no practical danger that a privacy protection culture would lead law enforcement to underestimate the need for surveillance or to act with excessive caution. There is a very real danger that, absent such a culture, any attempt to ensure effective accountability for all levels of law enforcement in this area will fail and the important right of privacy will be too easily overridden.

SUBMISSIONS AND COMMENTARY

I. DEFINITION OF 'COVERT SURVEILLANCE'

A. Starting Points

The proposed legislation is empowering legislation in that it purports to grant HK law enforcement agencies legal powers to carry out surveillance activities some of which, in the absence of such legislation, several HK courts have declared to be unlawful – at least in the sense of being inconsistent with the rights of privacy protected by the Basic Law. This would suggest a definition of covert surveillance that is relatively narrow and confined, thereby confining permitted surveillance within acceptable bounds.

However, the HK government takes the view that many forms of surveillance not covered in the legislation are lawful notwithstanding the Basic Law protection of privacy because (i) according to our domestic law ordinary citizens are not prohibited from carrying out such forms of surveillance and law enforcement agencies should not be subject to greater restrictions that private citizens and (ii) these other forms of surveillance are in any case not sufficiently intrusive of person, property or privacy to be disproportionate to their legitimate objectives.

Therefore, exclusion of a form of covert surveillance from the proposed legislation would not mean that law enforcement agencies regarded that form of surveillance was unlawful and ought not be engaged in. They – and the courts – are much more likely to operate on the understanding that forms of surveillance not covered by the legislation that are not otherwise punishable under the ordinary criminal law or as a tort, are perfectly lawful and can be used at an agency's discretion.

On the other hand, the proposed legislation is restrictive and regulatory in that it purports to limit and regulate HK law enforcement agencies' use of some forms of surveillance which surveillance, though widely used, was previously effectively unregulated, or at best only self regulated. It is submitted that, given the present state of the legal environment in which this legislation would operate where specific legal protection of privacy is limited at best, it is essential that the

definition of covert surveillance within the legislation be as wide and comprehensive as possible consistent with the boundaries of the concept.

In considering those boundaries, the question we should ask is whether as a free society the surveillance activity is activity we would want someone outside the LEA community, someone like a panel judge and/ or the Commissioner, to know and approve in advance, or at least know of and review ex post facto. If we would want someone else to know about that activity then it has to be covered by the ordinance.

In this context it is important to appreciate that although it is essential that all prior authorization and ex post facto authorization requirements are backed by mandatory reporting and accountability obligations, it is certainly not necessary and, we would argue not desirable, that mandatory reporting and accountability obligations should be restricted to authorization cases.

SUBMISSION 1:
The definition of 'covert surveillance' should be as wide and comprehensive as possible consistent with the boundaries of the concept and, in particular, should include all covert surveillance activity we would wish to be subject to at least reporting and monitoring by our agents outside the LEA community.

B. 'With the use of any surveillance device'

'Covert surveillance' is confined to surveillance using one or more surveillance devices, i.e. 'a data surveillance device', 'a listening device', 'an optical surveillance device', 'a tracking device' where 'device' 'includes any instrument, apparatus and equipment'.

Generally speaking, the Administration's argument that confining the provisions to surveillance using something other than the unenhanced (or ordinarily corrected) senses of a human being in public places is impractical/unnecessary seems plausible. The arguments that (i) other jurisdictions do not require prior authorization for surveillance without devices and (ii) LEAs who engage in covert surveillance without devices in private premises would be liable for tortious trespass are not impressive.

However, there are instances of surveillance without the use of a device of which

we would want our independent monitors to be aware.

As to surveillance without the use of surveillance devices in a public place:
the Administration argued at para 9 of * that *"where there is a reasonable expectation of privacy [in a public place] it is not possible to keep the surveillance covert [without] ... alerting the persons [subject] to the surveillance, without using a device."*

With respect, this is not so. Please refer to the discussion of 'reasonable expectation of privacy' and 'public places' below.

As to covert surveillance without a device in private premises, Para 9 included the following:
"If an activity takes place in private premises, the LEA's will be liable for trespass under the common law as well as for any unlawful act that they may carry out on the premises if they enter premises without unlawful authority. Our LEA's would not carry out unlawful activities."

Perhaps, although if the latter sentence is really true, comparison with data from other jurisdictions would suggest a level of restraint amongst HK LEA's that is unique. There is also the point that post Basic Law it is very possible that covert eavesdropping inside private premises is now unlawful (though not of course criminal) – but surveillance without a device inside private premises need not be confined to eavesdropping.

It could include opening a computer, searching and reading its files manually (that is, without the aid of another computer or special software and hence not using a data surveillance device). Or opening briefcases, safes, drawers, filing cabinets etc, even reading documents on a desk. All this conduct would be problematic and is certainly activity of which we would want our independent observers to know – and preferably to have authorised.

With respect, residual liability for tortious trespass is no answer to this point – even if bringing an action for trespass should become a practical reality in the future. Such liability is also available for people who trespass in order to plant surveillance devices and is not thought sufficient to deal with them. Why should the additional act of photography or recording make all difference between uncontrolled secrecy and accountability?

It is noteworthy that the Law Reform Commission specifically proposed that 'use of a technical device should NOT be a necessary ingredient' of their proposed

offence of trespassing 'with intent to observe, overhear or obtain personal information' – see LRCHK Report on Privacy: The Regulation of Covert Surveillance, para 1.10.

SUBMISSION 2:
'Covert surveillance' should not be restricted to surveillance using surveillance devices.

SUBMISSION 3:
'Covert surveillance' should not include observation or eavesdropping in public places unassisted by surveillance devices arising other than in pursuance of a pre planned targeting of an individual, group of individuals or place.
[Pre-planned means planned before the person observing or eavesdropping identified the intended target.]

C. 'Systematic' surveillance only

As a matter of language:

In Response to Issues Raised at the Bills Committee Meeting held on 9 May 2006, available as LC Paper No. CB(2) 2010/05-06(01), the Administration proposed to delete 'systematic'.

This is a linguistic improvement. 'Systematic' suggests a distinction between ad hoc, one off surveillance and longer term activity, but that is not a principled distinction that the recognized public interest in protecting privacy rights would invite us to make and does not appear to be the distinction the Administration intended. The term is inappropriate for an attempted distinction between surveillance activity of what ever duration that must be initiated immediately because of operational circumstances ("this is our only chance to get a tracking device on that suspect's vehicle") and similar activity that for which there is time to seek at least oral authorization, which does seem to be the distinction the Administration had in mind.

As a matter of policy:

The Administration proposed expanding para (b) of the definition to include '(i) any spontaneous reaction to unforeseen events or circumstances' as an

alternative way of achieving their objective, i.e. to permit spontaneous surveillance where even oral prior authorization was impractical because of time constraints.

But is the exclusion of spontaneous surveillance activity from ALL aspects of the legislation – the inevitable result of excluding spontaneous surveillance from the definition of covert surveillance – desirable as a matter of policy?

Granted that LEAs must sometimes act immediately so that PRIOR authorization is impracticable, that does not mean that EX POST FACTO authorization/ reporting/ monitoring should be abandoned also. Why is spontaneous surveillance any less in need of monitoring than emergency or oral application surveillance?

In the Administration's Response to Submissions to Bills Committee, published as Annex B to LC Paper No. CB(2)2198/05-06(01), the Security Bureau, responding to concerns expressed by the Human Rights Monitor, at item 20 said,

> *"The qualifier [systematic] is necessary to exclude immediate response to operational circumstances or cursory checks that form part of an LEA officers' routine operations, e.g., in the course of patrolling a public place."*

What kinds of immediate responses or cursory checks did the Administration have in mind?

First, they must have involved covert use of surveillance devices since, contrary to SUBMISSION 2 above, such use is a necessary prerequisite for coverage by the Bill.

Second, operational circumstances might require **immediate** use of a wide range of surveillance activities in circumstances of real emergency and/ or fast moving events, eg **immediate** planting of listening/ tracking devices on suspects, cars etc, sending in someone fitted with a wire, using devices to search through computers, in each case trying to prevent imminent specific serious crime or other specific dangerous events or, perhaps, save imminently at risk crucial evidence.

Third, they must have arisen in circumstances when even oral application to Head/ Deputy Head of Department for emergency permission re interception of communications or surveillance type 1 activity or authorizing officer re

surveillance type 2 activity is not possible/reasonable - that should surely be only in a very limited number of very extreme cases – really EMERGENCY emergency cases.

None of these characteristics suggest that spontaneous surveillance should be immune from the same ex post facto scrutiny as, say, emergency or oral application surveillance by reason of its spontaneity alone.

So spontaneous surveillance SHOULD be excluded from PRIOR authorization requirement but should NOT be excluded from EX POSTE FACTO authorization, recording and monitoring requirements as well as restrictions upon the use of any product thereby obtained.

Therefore, the inclusion of para(b) in the definition of "covert surveillance" is inappropriate. Section 5(2) would be a more appropriate place.

There is one further point.

Surely, as a matter of policy the exemption from even prior authorization requirements should only apply to NECESSARY spontaneous surveillance. Surveillance would be 'necessary' in this context where even telephone authorization is practically impossible without alerting the target, losing the target, losing crucial evidence and the relevant invasion of privacy would be proportional to the risk of the imminent commission of a serious offence, the evasion of detection, identification, arrest or conviction of the perpetrator of a serious offence.

SUBMISSION 4:
The term 'systematic' should be omitted from the definition of 'covert surveillance'.

SUBMISSION 5:
The proposed para (b) should not be added to the definition of 'covert surveillance. Rather section 5(2) should be amended to read:
(2) Subsection (1) does not apply to any covert surveillance carried out pursuant to a prescribed authorization or to any covert surveillance carried out as a necessary spontaneous reaction to unforeseen events or circumstances for which subsequent authorization was obtained pursuant to s. *.

The reference to section * reflects the consequential need for a separate section * specifically dealing with spontaneous surveillance and the need for subsequent reporting and authorization.

SUBMISSION 6:
Only necessary spontaneous surveillance should be exempt from prior authorization.

D. 'Where any person who is the subject of the surveillance'

What if no specific person is the subject of the surveillance but, rather, the whole purpose of the surveillance is to discover what is going on in a specific place, in a mosque for example? Or if the target of the surveillance is not a person but an organization, its aims and true intentions?

In the former case, the surveillance is not merely or primarily for the purpose of identifying who attends the mosque (then the persons attending might be said to be the subjects of the surveillance) but in order to discover what is being said inside the mosque. Would such surveillance require authorization? Should it? As a society, even though we personally may not be permitted to know, would we want a panel judge or our surveillance commissioner to know when law enforcement are monitoring our religious/ political/ commercial/ educational/ recreational gatherings? Or our clubs? We believe the answer is 'yes'.

SUBMISSION 7:
Surveillance of premises, places and organizations should also require authorization and be subject to monitoring etc.

E. 'A reasonable expectation of privacy'

This term is not defined, and it may well be true that it cannot be, but section 2(2) does provide that 'a person is not regarded as being entitled to a reasonable expectation of privacy within the meaning of paragraph (a)(i) of the definition of 'covert surveillance' in subsection (1) in relation to any activity carried on by him in a public place.'

Three points should be made here.

First, according to the Administration's responses, 'activity' is intended to apply to observable physical activity only, that is to the fact of presence and the fact of having a conversation with X in a public place, but not the substance of such conversation. However, the point is unclear and needs to be more expressly clarified.

SUBMISSION 8:
If the substance of the present section 2(2) is retained, it must at least be made clear that 'activity' does not include having conversation in a normal tone with specific persons.

Second, the definition of 'public place' in section 2 requires rethinking. 'Public place' is defined in part as follows:
"(a) means any premises which are a public place as defined in section 2(1) of the Summary Offences Ordinance (Cap. 228)".

'Premises' is in turn defined as including 'any place and, in particular, includes -
(a) any land or building;
(b) any conveyance;
(c) any structure (whether or not moveable or offshore)
..."

So clearly, the drafters intend that 'public place' includes some buildings and conveyances (presumably inside as well as out). But, in the context of 'public place', the wide definition of 'premises' is said to be circumscribed by the narrow definition in the Summary Offences Ordinance. That definition reads as follows:
"includes all piers, thoroughfares, streets, roads, lanes, alleys, courts, squares, archways, waterways, passages, paths, ways and places to which the public have access either continuously or periodically, whether the same are the property of the Government or of private persons'

Surely, the maxim *ejustem generis* invites the interpretation of the general words, 'and places to which the public have access ....' in the context of what has come before. If so, it suggests that such places might include public parks (since paths through public parks would seem to be included) but not buildings, certainly not buildings unconnected with spaces upon which or through which people move, and not conveyances that travel along such spaces.

[Is there contrary judicial authority? Even if there is, ordinary educated HK person should not be expected to know of it.]

Apart from the inherent clumsiness of defining such an important term by reference to another piece of legislation, clearly the definition of 'public place' in the Summary Offences Ordinance is inappropriate.

SUBMISSION 9:
The definition of public place should in any case be reconsidered and included in the Ordinance in full, without reference to other legislation, certainly not to the inappropriate provision in the Summary Offences Ordinance.

The third point is a matter of principle.

Is a person who is standing in a particular public place, talking to another person in a public place or traveling upon a public road 'carrying on an activity' in a public place?

If the answer is 'yes', then, according to ss 2(2) such a person cannot have a reasonable expectation of privacy as to the fact of their standing, talking or traveling (their activity) in that public place. Therefore, observing such people, even with the assistance of surveillance devices but not targeting their communications, cannot be covert surveillance within the meaning of subpara (a)(i) of the definition and is not covered by any protection within the legislation.

The position with respect to tracking is more obscure. The definition of Type 2 surveillance expressly refers to using tracking devices that do not require interference with any conveyance or object without permission. Now, use of an external tracking device to track a conveyance strongly suggests surveillance of a person's movement in, for example, a car traveling on a public road. So tracking an individual traveling on a public road in a conveyance is not covert surveillance but is Type 2 surveillance? The Administration apparently thought so, see Response to Issues Raised by Members at the meeting of 7 February 2006. With respect, that does not make sense.

As a matter of principle, we agree with the Administration that use of an external tracking device on a conveyance to track the physical movement of a person along a public road ought to be regarded as covert surveillance. But then the blanket exclusion of activity in a public place needs to be rethought.

With respect, the exclusion is in any case fundamentally misconceived. There is an initial appeal in the idea that a person in a truly public place such as a public park or road may not claim a reasonable expectation as to privacy re their presence in that place and their obvious physical activity within that place. But upon reflection, although this must be true with respect to observation by casual observers or even police officers on patrol, attributing to all an expectation of at least the possibility that they may be seen and recognized in a public place is a very different thing from claiming that a person has no reasonable expectation of privacy as to where they are going from the moment they set out from their front door until the time that they return to it. In fact, it is no longer even clear that a person cannot have a reasonable expectation of privacy as to their presence in a particular place, such as the entrance to a drug rehabilitation centre – *refer to the *Campbell* case. But certainly we all have a reasonable expectation that we will not be the subject of coordinated and sustained observation of our movements and activities by the authorities – with or without the use of surveillance devices. In fact, we may sometimes deliberately seek the anonymity that comes with inconspicuous presence within a large crowd.

Therefore, surveillance must include following a person on foot or by car in the old fashioned way as well as by using tracking devices. It must include staking out premises using only one's eyes and ears or with surveillance devices. If done by a private individual we might call it stalking, harassment if done by the paparazzi. When officials are involved it is surveillance.

Specific, coordinated targeted watching or persons or places is definitely something our independent monitors should know about and preferably authorize in advance.

SUBMISSION 10:
Remembering that permission to engage in such surveillance can be obtained by phone and that spontaneous following of suspects detected at the scene or unexpectedly is permissible, a decision to follow/ stake out a person or place should be treated as covert surveillance Type 2 even when that person enters a public place, including a public vehicle.

F. 'Is likely to result in the obtaining of any private information about the person'

The likelihood of obtaining private information about a person should be an important factor in any decision to commence covert surveillance but seems irrelevant as a matter of definition. Especially in a legal environment where surveillance is generally not specifically unlawful (that is, tortious or criminal as distinct from in violation of a protected human right), insistence upon such a likelihood would unduly narrow the reach of the legislative controls. The object of obtaining any private information about a person/ place is clearly at least as important as the chance of success.

However, it is certainly arguable that authorization should be sought even when obtaining private information is not the object of the surveillance if such is in any case a likely outcome.

SUBMISSION 11:
The phrase 'likely or intended' would be a better formulation.

II. DEFINITION OF 'TYPE 2 SURVEILLANCE'

If there is to be a division between different types of surveillance, subject to the under inclusiveness noted above, this is a sensible division. However, it should be made clear that this does NOT include any activity that would amount to civil trespass on the part of the person in paragraphs (i)A or (ii). If surveillance without the use of a device is included as a form of covert surveillance in future legislation, it should be classified as Type 2.

III. CONDITIONS FOR ISSUE, RENEWAL OR CONTINUANCE OF PRESCRIBED AUTHORIZATION.

A. Unnecessary complexity and rigidity

It is not necessary to split sections 3, 9 and 12 in this complicating and confusing way. Legislation elsewhere has one provision stipulating the test to be satisfied and the proper approach the judge/authorizing authority should take to the application of that test.

B. Legitimate Purposes

The Administration has suggested that 'obtaining evidence for proving the commission of a serious crime in a court' and fulfillment of HKSAR's mutual assistance obligations must be implied in the idea of preventing or detecting serious crime but, with respect, such an important matter should not be a matter of implication.

SUBMISSION 12:
Legitimate purposes for which interception or covert surveillance might be carried out should **explicitly** include 'obtaining evidence for proving the commission of a serious crime in a court' and fulfillment of the HKSAR's mutual assistance obligations.

[As to the relationship between this SUBMISSION and the effect of section 58 with respect to interceptions see discussion below.]

C. 'Public security'

As noted in LC Paper No. CB(2) 1866/05-06(02) para 7, prepared for 2nd May 2006, the Administration has indicated a willingness to confine 'public security' to 'public security of Hong Kong' and to require applicants for authorization to provide information as to, and panel judges to consider "an assessment of the impact, both direct and indirect, of the threat on[sic] the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong.". By including the word 'indirect', the Administration evidently intends the definition to be wide enough to undertake surveillance in accordance with our moral [reciprocal] obligations to monitor threats to other places outside HK – see para. 2(d). But this reading of the provision is hampered by the following phrases which tend to have a narrowing effect. It is submitted that specific references to 'residents' or 'other persons within HK' are in any case unnecessary.

If, in the future, HK's assistance is requested with respect to people who are a real threat to the public security of the greater PRC or some third jurisdiction, our law enforcement personnel will rightly wish to assist in gathering such information as they can – and should be **legally** able to do so to the full extent of our technical capabilities as is appropriate. This should be made explicit.

The proposed exclusion of protest activity is sound and should be as strong as possible.

SUBMISSION 13:
Specific references to 'residents' or 'other persons within Hong Kong' should not be included in any definition of "public security".

The words 'of itself' in the proposed para 5A should be omitted and replaced by 'to be'. [The qualification as to 'violent means' is already sufficient limitation.]

D. "Serious crime"

Query:
What offences are punishable by a maximum penalty that includes a fine of not less than $1,000,000 that are not also punishable by imprisonment of not less than 3 years? i.e. what offences is subpara (b)(ii) targeting?

The limit of not less than 3 years would permit surveillance with respect to unauthorized and unlawful assemblies under the Public Order Ordinance.
Since a threat of significant violence is not a necessary part of either of these offences – and given the concern that surveillance of peaceful dissent should not be permitted – this is objectionable.

SUBMISSION 14:
The offences relating to unauthorized and unlawful assemblies in the Public Order Ordinance should be expressly excluded from the definition of "serious crime" for the purposes of Type 2 surveillance.

NOTE: If this has the consequence that the police are no longer able to photograph peaceful protests, so much the better. Participation in a peaceful protest should not be a matter of concern to those interested in law enforcement or public security. It is precisely the kind of information public authorities ought not to be permitted to keep on record.

E. 'Balancing'

There is danger in the use of the term 'balancing' – especially largely unguided balancing between various factors to which the judge/ authorizing officer is free

to give such weight as she sees fit. Previous experience with balancing tests, especially in the common law world suggests such a formulation is likely to lead to an all too ready appraisal that the intrusion into the protected right of privacy is justified.

The idea of balance may invoke an image of a set of scales in the form of a pole, with baskets at either end balanced on a fulcrum. With at 'large balancing', the pole starts in the level position. Factors for and against the application are placed in the relevant baskets, with the judge deciding how much weight to assign to each factor (three pounds of public safety, five pounds of collateral impact on non targets etc). There is also a kind of 'weighted balancing' that starts with the protected right weighing down its side of the pole with the applicant's basket initially high in the air and empty. The party who seeks authority to limit that right then has to place weighty evidence and special circumstances and need in the empty basket sufficient to alter the balance of public interest in favour of **the need for and proportionality of the specific limitation in the specific circumstances of the individual case** in order to succeed. It is still possible for an insensitive or prosecution minded judge/ authorizing officer to give the right of privacy away too easily – that is why the need for records and ex post facto justification and accountability remain so important – but at least there is the privileged weighting in the privacy basket that must be overcome first.

There is undoubtedly a strong public interest in the detection, prevention and prosecution of serious crimes. However, there is also a very strong public interest in the protection of our private communications and private homes, offices etc from the prying eyes of government – it is that interest that is given fundamental protection by the Basic Law and the BOR.

Interception of communications inevitably completely negates a right of privacy with respect to those communications. Use of surveillance devices within private premises likewise invariably destroys the privacy of those premises – for all the occupants. Not intercepting communications and not using surveillance devices within private premises does not have the same automatic impact upon any of the legitimate purposes for using such methods – although the practical effect may be to prevent law enforcement from detecting or preventing a specific serious crime in some circumstances.

This disparity in impact should mean an initial starting point that interception or covert surveillance will not be authorized unless that law enforcement agency

can clearly establish the necessity and proportionality of the proposed activity to the reasonable satisfaction of the judge/ authorizing officer.

This is the formulation/ standard typically required for justification of violations of human rights. No basis for applying any lesser standard to the protected right of privacy has been demonstrated.

SUBMISSION 15:
The whole structure of clause 3 should be revised – and simplified.

The term 'balancing' should be avoided.

The authorizing provision should in terms state that authority for interception/ covert surveillance **will not be granted unless** the judge/ authorizing officer, having carefully considered the specific aspects of the privacy right being challenged (not merely but including the degree of intrusiveness) and the specific circumstances of the applicant's case (not merely but including the factors set out in clause 3 as it now appears) is satisfied that the government has established the need for and proportionality of the specific limitation requested.

F. 'In operational terms'

The use of the phase 'in operational terms' suggests a weighting in favour of the needs of law enforcement – there is certainly a danger that the phrase will be so interpreted. The Administration's explanations of the perceived need for the term have been unconvincing. Of course any authorizing judge or officer or the Commissioner will consider the operational needs of law enforcement in the circumstances. Subpara (ii) would require such consideration in any case. But there should be no suggestion that operational needs should have extra weight.

SUBMISSION 16:
Even if, contrary to the above, the present structure is retained, the phrase 'in operational terms' should be omitted.

[The Administration's willingness to alter this language was indicated in the press but I have been unable to track down the details as yet.]

G. 'Relevant factors'

The list of relevant factors is much too limited.

Furthermore, the list of 'relevant factors' in subsection 2 should not be exclusive, as the use of the word 'means' suggests that it is.

In any case and especially if the present exclusivity of factors is retained, the judge/ authorizing officer should expressly be required to consider the quality (reliability and sufficiency) of the evidence upon which the law enforcement agency has selected or suspects the particular target as a separate relevant factor. If the judge/ authorizing officer is not required to ask for and carefully evaluate the information upon which the law enforcement agency seeks permission to act, the whole authorization exercise is likely to prove rather formal and automatic. The mischief, as they say, is in the detail and, in this context, the detail is the quality of the original intel. The full force of our most intrusive forms of surveillance may well be proportional when we have reasonable grounds to suspect that a target is a member of a terrorist cell – even without any grounds for suspecting they are actually planning to do anything in HK – but no surveillance of any kind would be proportional if our only source of information was a match between the target and a 'potential terrorist profile' of 'male, muslim, between 18 and 40, has visited/ was born in Afghanistan/ Pakistan/ Saudi Arabia/ Iraq/ Iran/ Syria'.

So the judges/ officers should be required to ask the question, "And you believe this because?" and to be satisfied as to the sufficiency of the answer. A mere 'we have information that' ought not to be sufficient. Accepting the applicant's word that he has reasonable grounds to believe is no supervision at all. It is precisely the reasonableness of the grounds that must be tested.

It might be argued that the requirement that the judge/ officer consider 'the immediacy and gravity' of 'the serious crime' or the 'particular threat to public security' implies that the applicant must supply the judge/ officer with the facts needed for the judge/ officer to be able to make that determination. How can the judge assess the immediacy of an offence without looking at the evidence the applicant has about probable commission of the offence by the alleged target? Surely, the need for such evidence is obvious.

Perhaps – but we are concerned that it is not in fact sufficiently obvious. We believe the point should be made expressly so that there is no room for doubt.

Of course, the need to consider 'the likely value and relevance ... of the information likely to be obtained by carrying [out the surveillance or interception]' in sub paragraph (b) does not cover the point. There is a fundamental difference between the value and relevance of what one would expect to find if one has correctly identified the planner or perpetrator of a serious crime (which should certainly be a factor the authorizing judge/ officer considers!) and the quality of the evidence upon which the law enforcement agency has come to believe – or reasonably suspect – the target is such a planner or perpetrator or someone associated with a planner or perpetrator as the case may be.

SUBMISSION 17:
The panel judge/ authorizing authority/ should be specifically required to consider the quality (reliability and sufficiency) of the evidence upon which the law enforcement agency relies in selecting the surveillance target and advocating the need for surveillance.

NOTE: The structure of the legislation does not expressly require the requesting officer, or approving directorate officer to believe, or reasonably believe anything – let alone demonstrate the reasonableness of an honestly held belief to anyone – cf the conditions for issuing a search warrant.

That deficiency would also need to be corrected. See below.

NOTE: Totally innocent residents of a society that values social stability (such as most of the residents of HK) may be assumed to accept the risk that they could be the subject of communication interception or covert surveillance by officers acting in good faith upon evidence of acceptable quality – a reasonable suspicion remains a reasonable suspicion at that time, not withstanding the target's innocence is conclusively established at some later time. But HK residents cannot be assumed to accept the risk that they will be the subject of communication interception or covert surveillance by officers not acting in good faith or by officers acting in good faith but on the basis of poor quality evidence such as the unsubstantiated evidence of a mentally retarded person proved unreliable in the past.)

One function of directorate level officer and judge/ authorizing officer must be to act as an additional check on quality of law enforcement decisions as well as to

ensure that privacy is given its appropriate value. These are two sides of the same coin.

IV CLAUSES 4 and 5

Prohibitions without legal sanctions are an anathema to the common law – and for good reason. Just as a person does not have a true right until there is an obligation upon others to respect it, backed by a legal cause of action to compel such respect if necessary, so is a person not truly prohibited from action until others are empowered to prevent that act and there is a legal cause of action (civil or criminal) to enforce the prohibition or at least ensure compensation/ sanction for its breach.

Unless a court seizes the initiative to treat them as a basis for a specific new tort – or breach of the rights protected by the Basic Law is recognized as the basis for a cause of action + appropriate remedies including compensation – the prohibitions in sections 4 and 5 are meaningless.

That would be unfortunate. Breach of this legislation would likely mean violation of a constitutionally protected human right for which existing laws otherwise provides only patchy and largely ineffective remedies. The Administration has relied upon the narrow function of the proposed legislation to explain that it would not be fair to subject law enforcement personnel to criminal sanctions without applying the same laws to private institutions or individuals. Since the legislation is not intended to deal with private surveillance, generally applicable offences would be outside the scope of the legislation. Hence, in the interests of maintaining parity, it would be better not to create any criminal offences at all – at least for now.

Perhaps criminal offences are not the answer, at least in the absence of proof of mala fides. But tortious liability, with appropriate principles of vicarious liability, seems entirely appropriate – even if confined to law enforcement personnel. As noted in LEGCO, the recent HL decision in *Watkins v Home Office and others* [2006] UKHL 17 suggests the tort of misfeasance in public office will often be inappropriate because of the complainant's inability to prove material damage – so something more moulded to the particular circumstances is required. This is particularly so when it is remembered that, if this Bill is passed,

the potential for legal surveillance by law enforcement agencies will be very wide. There would really be no excuse for breach.

SUBMISSION 18:
Breach of the prohibitions in sections 4 and 5 should provide a sufficient basis for an action in court – with appropriate remedies available such as the destruction of information, apologies and compensation.

V JUDICIAL AUTHORIZATION

A. Section 8

Section 8 provides that an officer may apply for judicial authorization for Type 1 surveillance 'in writing' and supported by an affidavit in accordance with Parts 1 or 2 of Schedule 3.

According to that schedule, information that must be included in the affidavit includes:

- the legitimate purpose for which the authorization is sought
- the form of proposed interception / Type 1 surveillance and the information to be obtained thereby
- identity of target **if known**
- particulars of addresses, premises, numbers, apparatus, objects (class) etc on, in or with which task to be carried out **if known**
- proposed duration of interception/ surveillance
- the nature of the serious crime/ threat to public security
- an assessment of the immediacy and gravity of the serious crime/ threat to security
- the benefits like to be obtained by carrying out the interception/ surveillance
- identities/ description of and assessment of impact (if any) on person (class of person) other than the target who may be affected
- likelihood information subject to l.p.p. will be obtained
- reason why purpose sought to be furthered by intercept/ surveillance cannot reasonably be furthered by other less intrusive means
- name and rank of applicant

As the words 'if known' indicate, there is considerable room for variation in levels of detail – and conspicuously lacking from the list is a clear statement of the need to **show** as distinct from assert reasonable grounds for targeting the particular person – that is, the judge appears to be required to accept on faith the quality of the law enforcement intel. Of course, there is nothing forbidding the applying officer from including such a showing – and no doubt many judges would ask and receive – but there is no clear command that such a showing is required.

Is that the situation intended? Should such secrecy be allowed? Surely the specially vetted panel judges' discretion can be trusted with such information. The whole point of the authorization system is that the law enforcement agencies should not be left as a law unto themselves. There is a need for outside judgment, supervision and accountability. To be effective, that judgment, supervision and accountability must extend to the adequacy of the law enforcement agency's intel.

SUBMISSION 19:
Applicants for authorization should be required to show that they have reasonable grounds for their honest belief that the proposed surveillance of this particular target is necessary and proportional in pursuit of one of the legitimate objectives.

Judges/ authorizing officers should be required to be satisfied as to the existence and validity of those reasonable grounds.

VI EMERGENCY ATHORIZATIONS

A. The Occasional Need for Emergency Applications

The occasional need for emergency applications seems clear. Subsequent confirmation of emergency authorization is essential. The panel judge's examination of the circumstances should be fair, practical but rigorous.

B. Who is the Head/ Deputy Head of a Department?

In section 2, 'department' is defined as a department specified in Part 1 and/ or 2 of Schedule 1. So the head of a department is, for example, the Commissioner of Police or the * of the ICAC. The position with respect to Customs and Immigration is perhaps a little less certain. Does the term refer to the relevant Secretary or to the civil service head?

Since the contents of Schedule 1 can be varied by the Chief Executive, it seems preferable and not be too much trouble to be more explicit as to the titles of the relevant heads.

C. Loss of Vital Evidence

Section 20(1) is the first EXPLICIT reference to loss of vital evidence – a clear indication that obtaining and preventing the loss of evidence of crime is thought to be part of preventing and detecting crime. With respect, given the history of interception in UK and HK and the current legislation in UK that spells out obtaining evidence as a legitimate objective of surveillance quite expressly, this view may not be correct – or at least not universally shared. As noted above it would be better to make the point clear and at a much earlier stage in the legislation.

VII ORAL APPICATIONS

A. General Support

The rare need for oral applications is also clear – even at the authorized officer level since circumstances on the ground may change very fast. In fact, from a human rights perspective, an oral application to a panel judge may well be preferable to a written emergency application to a head of department. If the ultimate safeguard against abuse is accountability, the oral application to the panel judge has the advantage of having knowledge of the proposed activity outside the agency 48 hours before it otherwise needed to be – and precluding subsequent deliberate or negligent concealment within the agency. Subsequent confirmation would be required.

B. Automatic disposal of information obtained from interceptions/ surveillance carried out pursuant to emergency/oral authorizations not subsequently confirmed

It is not necessarily desirable that the information obtained by means of emergency/ oral intercepts or covert surveillance be destroyed unilaterally by the relevant head of department whenever an application for confirmation of the emergency/ oral authorization has not been made within the 48 hour period.

No doubt the intention here is protection of privacy of those improperly subject to interception/ surveillance and provision of an additional incentive to relevant officers to comply with application for confirmation requirements.

But where accountability is an important safeguard against abuse there is a strong case for preserving the information at least for the prompt examination of the Commissioner – and perhaps for use by any complainant should a claim against an agency be appropriate.

SUBMISSION 20:
Surveillance product obtained by interceptions or surveillance conducted pursuant to [spontaneous], emergency or oral authorizations where no subsequent authorization was obtained within the requisite time period should not be destroyed until so ordered by either (i) a panel judge or authorizing officer (where application was made but rejected) or (ii) by the Commissioner (where no application was made).

Such surveillance product should be sealed and not available for use by any LEA unless otherwise authorized by the Commissioner.

VIII The Commissioner

A. The Primary Importance of the Commissioner to the Effectiveness of the Scheme

As previously stated, knowledge and accountability outside the agencies is crucial to effective protection of privacy against unwarranted/ arbitrary/ abusive interception and covert surveillance. An independent, pro-active and powerful

Commissioner (powerful in the sense of possessing full investigation and follow up powers and effective teeth for the enforcement of those powers) is essential to effective accountability.

B. The Commissioner and the Panel Judges

The Commissioner's supervisory role should extend to oversight of the work of Panel Judges, not just the departments and their officers. Such oversight would not threaten the independence of the judges. On the contrary, it may help protect it. There is a danger that a judge might become conditioned to applications from the agencies and perhaps begin to see the agency's point of view a little too easily. The need to prepare a report – or to explain specific decisions to the Commissioner should reduce that risk.

Of course, the Commissioner should have no authority to influence a panel judge's decision with respect to a particular application – or even to dictate policy etc. The Commissioner's function would be strictly monitoring with respect to the panel judges.

NOTE: much of the information required for the monitoring of the Panel Judges would be needed for the annual reports to the Chief Executive required by clause 47. However, the Commissioner's monitoring function should be more proactive than simply receiving and passing on statistics prepared by the judges. The proper protection of our rights of privacy may require the Commissioner to actively review the records and practices of the specific panel judges. The Commission should be able to demand access to more specific information, including information about a particular case for this purpose as required.

SUBMISSION 21:
The Commissioner's monitoring functions should extend to actively monitoring the decisions of the Panel Judges.

SUBMISSION 22:
The Commissioner should be selected from past/ present judiciary above the rank of the Panel Judges. i.e. at least at appellate level.

C. The Commissioner's Powers in Relation to an Examination

Requiring the Commissioner to apply principles applicable on an application for judicial review is much too restrictive for an essential monitoring function.

At the initial stage of establishing the facts, the Commissioner should have full investigatory/ inquisitorial powers. **The statement that the Commissioner should carry out the examination on the basis of written submissions made to the Commissioner is totally unacceptable.** Such a requirement would leave the enforcement agencies as masters of their own houses. The whole point of the legislation should be to ensure that that does not happen – that there are panel judges and a Commissioner who are out side the agencies and independent of the agencies political masters, who know exactly what the agencies are doing or who, in the case of the Commissioner, can ferret around until he does. It is very clear from very recent history elsewhere that intelligence gathering can become a self legitimizing and very dangerous activity if left unattended. It is impossible for 'the people' to supervise covert surveillance directly. But it must be supervised – and supervised on the people's behalf by independent, totally trusted and very powerful independents.

The object should be to get at the truth. There must be no secrets from the Commissioner. The Commissioner must have sole responsibility for determining what the Commissioner needs to know in a particular case – there must be no obstruction, no protection of the agency etc.

SUBMISSION 23:
When an application for an examination has been received, the Commissioner must have the responsibility and all the necessary investigatory powers to determine the questions of fact raised by the examination.

At the second stage, when the facts have been established and the Commissioner must determine whether interception/ covert surveillance that required an authorization but what not authorized has occurred, the analogy with judicial review is more appropriate but still not apt. Even if the judicial review is of the modern, post human rights variety, it is still not sufficient to enable the Commissioner to carry out his monitoring function. The Commissioner is not merely concerned with the technical legality of the individual case. The Commissioner should be concerned with the bigger picture, with questions of

policy, culture and fairness. The complexities of judicial review – and they are many – are an unnecessary burden here.

SUBMISSION 24:
The Commissioner's determination as to whether upon the established facts a communication transmitted to or by a person seeking an examination has been intercepted or such person has been subject to covert surveillance otherwise that pursuant to a RELEVANT, VALID AND CURRENT PRESCRIBED AUTHORISATION should not be hampered or complicated by the complex rules and sometimes artificial limitations of judicial review.

D. The Commissioner's Powers to Acquire Information

Clause 51 gives the Commissioner powers to order officers (or any other person) to answer questions or provide information or, in the case of officers only, to prepare reports 'for the purpose of performing any of his functions under this Ordinance'.

SUBMISSION 25:
The powers under clause 51 should expressly extend to the fact finding stage of the examination process.

The Commissioner's orders under this section should be in the nature of a judicial warrant and should be enforceable in the same way as a warrant.

Failure to produce a requested report should be a serious disciplinary offence, arguably a criminal offence analogous to a contempt.

Failure to produce a requested report should require the Commissioner to conclude appropriate issues of fact against the relevant LEA, for example, that the relevant procedures were observed, that the relevant officers acted in good faith etc.

E. The Commissioner's Power to Recommend Disciplinary Action against specific officers

The Commissioner does not expressly have a power to include such a SUBMISSION in the notification to a head of department of a particular determination. Such a power should be expressly included and a head of department who decides not to follow that SUBMISSION should be required to explain why very specifically in the follow up report.

There need not be a witch-hunt or scape-goating action whenever an error, even an egregious error, occurs but agency officers and seniors must NEVER be permitted to develop the believe that breach of the rules doesn't really matter because even if they break the rules, nothing happens. Or just a rap on the knuckles perhaps.

In committing to this legislation, the Government and the legislature (the people?) are committing to a certain set of priorities. Remembering that it has previously been stressed that the agencies must be legally able to do what ever they reasonably need to do to save lives etc, it is not for the agencies to re-order those priorities. Not even when acting with the genuine belief they act in the best interests of the people. The whole point of this legislation is that no one is to be permitted to be a law unto themselves – not even in the interests of national security.

The law provides for the possibility of emergencies – and the law provides for at least subsequent accountability and that accountability should come complete with sanctions if need be. Sanctions that reach as high as the chain of command if necessary.

SUBMISSION 26:
The Commissioner should have an express power to recommend disciplinary action against specific individuals to their respective Heads of Department or, if a Head of Department is a target of the SUBMISSION, to the Chief Executive.

Failure, refusal to follow the SUBMISSION must be expressly and promptly explained to the Commissioner.

VIII Non-admissibility of Telecommunications Interception Product

A. Inadmissibility of the Product Itself

Section 58(1) provides that telecommunications interception product is not admissible in evidence before any court other than to prove [an offence constituted by the disclosure of telecommunications product or any information derived there from].

Note: Does 'prove' include 'disprove'? Certainly what is available to the prosecution should be available to the defence.

The restriction is too absolute. If the purpose is to conceal the technological capabilities and practices and procedures of inercepters, there are other ways.

First, it is extremely doubtful that the prohibition should apply where there is no question that the interception was made – for whatever reason, the prosecutor and defence already know it was made. If that is so, it seems unlikely that use of the material could reveal technology or methods of which the defendant was not already aware. If the product is incriminating, the prosecution should at least reserve to itself the possibility of using the product as evidence should that prove advisable. If the product is at all exculpatory there may well be unfairness, certainly there will be perceived unfairness, in withholding evidence that might assist the defence. If there is a dispute as to the content of a communication, the court is denied the best evidence upon which to decide the issue. Even worse, the defendant is driven into a credibility contest at which s/he is all too likely to be at a disadvantage.

The latter at least is a situation in which the judge might be expected to order disclosure of the tape to the judge pursuant to clause 58(4) – and then to require stipulations by the prosecution as to the content of the communication if that should be appropriate.

What if the fact of the interception is not known – should the government tie its hands so that even if the product from the interception could secure the conviction of a dangerous criminal, without revealing anything of which an intelligent offender was not already well aware, the government would have no choice but to let the criminal walk free?

What of the less likely situation that the product might be of significant assistance to the defence? There might, for example, be a dispute about what was said during a particular telephone conversation but the defendant is unaware of the product that could determine the issue. Should the government be permitted to withhold it? It is one thing to say the government may choose to try and win a prosecution without an informant's evidence or an intercept product. It is quite another to say they may proceed with a prosecution whilst withholding evidence they know would/ might assist the defence. That latter would not be a fair trial.

In this latter case, it is also less likely that a judge would order disclosure to the judge since the judge would not know of the interception.

SUBMISSION 27:
There should not be any absolute bar on the use of the product of an interception in a criminal trial.

The government should always have a discretion to release product for use in a criminal trial to the prosecution and/ or the defence – just as they may decide to use evidence of an informant or not.

The prosecution must disclose the existence of any product that may assist the defence to the trial judge.

A trial judge should have the power to order disclosure to the judge as contemplated in the Bill, except that the requirement of satisfaction that disclosure is 'essential in the interests of justice' before the judge has even seen the product is too high a test.

The prosecution must have the right to abandon the prosecution rather than disclose the product as ordered by the judge.

The trial judge may review the content of disclosed product and order the prosecution to stipulate to certain facts in the manner currently envisaged.

M Jackson
Associate Professor
Faculty of Law, HKU

J Brabyn
Lecturer
Faculty of Law, HKU