LC Paper No. CB(2)259/05-06(01)

Surveillance, Basic Law Article 30, and the Right to Privacy in Hong Kong

-- A Briefing Paper

October 2005

HONG KONG HUMAN RIGHTS MONITOR

4/F Kam Tak Building, 20 Mercer Street, Sheung Wan, Hong Kong
Phone: (852) 2811-4488 Fax: (852) 2802-6012 Email: contact@hkhrm.org.hk

Acknowledgments

This briefing paper was researched and written by Tom Kellogg.

The author wishes to acknowledge the helpful comments of ***Law Yuk-kai***, ***Kit Chan***, ***Philip Dykes***, ***Naz Modirzadeh,*** and ***Benton Olmsted***.

Surveillance, Basic Law Article 30, and the Right to Privacy in Hong Kong

Contents:

I. Summary and Recommendations

On April 22, 2005, Judge Fergal Sweeney issued a decision in the District Court of Hong Kong at the end of a *voir dire* hearing – a mini-hearing in the course of a trial held to determine whether certain evidence against the accused should be admitted – that resonated well beyond the case at hand. On the surface, there was nothing particularly special about the case, a criminal prosecution of four Hong Kong businessmen for attempted bribery by Hong Kong's Independent Commission Against Corruption, or ICAC.[1]

But the case revealed a gap in Hong Kong law, left over from Hong Kong's British colonial days, and never addressed by the post-1997 government during its nearly eight years in power. The ICAC, in the course of a routine investigation, engaged in covert surveillance of the suspects during their investigation, recording two conversations between the suspects at two different Hong Kong restaurants. In the absence of any law authorizing covert surveillance, the ICAC had no power to engage in such activity. Although Judge Sweeney allowed the evidence to be used and for the prosecution against the men to go forward, he warned that future use of covert surveillance without any legal authority would be suspect. In other words, the ICAC, and also the Hong Kong police, were living on borrowed time.

In fact the gap in the law was well-known to both the government and to a small group of legislators who followed the issue closely, some of whom had been pushing the government to act for years,[2] but the public was generally unaware of the problem. And, until Judge Sweeney's decision, as well as a decision issued in a similar case before another court less than three months later, the government felt no immediate obligation to do anything about the situation.

After the two court decisions, the government had no choice but to respond. If it did nothing, police officers and ICAC investigators might be reluctant to engage in any form of covert surveillance, and any ongoing or future investigations of corruption, drug smuggling, or triad activity might grind to a halt.

Unfortunately, the government's response created more problems than it solved. On August 5, 2005, the Chief Executive issued an executive order – to be followed, eventually, by proposed legislation, according to the government – regulating covert surveillance by the Hong Kong authorities.

Under the Executive Order, surveillance can only be carried out after being authorized by a sufficiently senior officer of the department, one specially designated by the department

[1] *HKSAR v. Li Man Tak and Others*, 22 April 2005, [2005] HKEC 1308.

[2] At least as early as 1987, legal scholars had pointed out that Hong Kong had no law restraining or otherwise regulating the government's use of covert surveillance. Several times since then, the topic has been raised, and opportunities to deal with the issue have come up, most notably in 1996, with the release of a lengthy and comprehensive Hong Kong Law Reform Commission study of both interception of communications and covert surveillance. But despite these several entreaties, the government, both before and after 1997, did nothing.

head to review such requests.[3] Although each department head must also name a second officer to periodically review authorizations under the Executive Order, no mechanism was created to allow for external review, and no other procedural safeguards were put in place.

In addition to creating a framework for authorizing surveillance for the investigation of common crimes, the Executive Order also covered electronic surveillance for the purpose of "protecting public safety or security,"[4] without any further definition of the term provided. This provision raised concerns that the government was attempting to create a legal framework for political surveillance – the surveillance of peaceful political activists – in the name of protecting security.

With the Order, the Chief Executive stepped into an area that, under the Basic Law, must be dealt with through legislation. The order purported to be an act of lawmaking, something that only the Legislative Council is empowered to do. Until legislation is introduced and the order is withdrawn, the Chief Executive has thrown the constitutional structure of Hong Kong off balance.

The court decisions, and the ensuing Executive Order, have revived a debate that had been stymied by the government's repeated protestations, made over several years, that it needed more time to "study" the question of covert surveillance. The government has since promised new legislation to be introduced in early 2006, most likely to cover not only covert surveillance but electronic surveillance more generally, including interception of communications.[5]

According to the government, the need to act quickly was a central motivation behind the use of the Executive Order. But there were other options at its disposal: the government could have worked with the Legislative Council to pass emergency legislation, with the

[3] Law Enforcement (Covert Surveillance Procedures) Order, Part 5, Section 15, July 30, 2005.
[4] Law Enforcement (Covert Surveillance Procedures) Order, Part 1, Section 3(a)(ii).
[5] The technical legal terms for various means of electronic surveillance are very different from those that are in common usage, and can be the cause for some confusion. In this paper, Hong Kong Human Rights Monitor uses the term "electronic surveillance" to refer to any form of surveillance of individuals that is aided by electronic instruments. "Interception of communications" refers primarily to the tapping of an individual's phone or fax line or other forms of electronic communications, but has historically also referred to the intercept of more low-tech communications, including handwritten letters sent through the mails. "Covert surveillance" generally refers to forms of electronic surveillance other than interception of communications, including bugging an individual's apartment or office, secretly recording conversations in public places, or arranging for one participant in a conversation to wear a recording device, or "wire" in order to capture the content of the conversation. Interception of telecommunications is currently covered by legislation, specifically Section 33 of the Telecommunications Ordinance, but that law provides little in the way of safeguards against government abuse. Interception of postal articles is covered by Section 13 of the Post Office Ordinance which suffers from similar problems. The Interception of Communications Ordinance enacted but not yet brought in force seeks to repeal these two problematic provisions and to introduce a court order system to authorize interception of any communications in the course of its transmission by post or by means of telecommunication system through the use of any electro-magnetic, acoustic, mechanical or other device. Interception of communications is discussed in more detail below.

appropriate sunset provisions, to cover the gap in the law while permanent legislation was in process.[6]

While the government's resolve to act after years of delay is welcome, Hong Kong Human Rights Monitor has serious concerns about what the government has already done, and what it may attempt to do with its legislative proposals, which, according to one Security Bureau official, are now the Security Bureau's "top priority."[7]

These concerns are based in part on the government's long record of seeking to weaken human rights protections in Hong Kong law. Just after the 1997 handover, the central government in Beijing used its power under Article 160 of the Basic Law to weaken the human rights protections of several key laws, including the Societies and Public Order Ordinances. In 1999, the SAR government invited an "interpretation" of the Basic Law, Hong Kong's mini-constitution, by Beijing in the so-called right of abode case. Beijing's interpretation ushered in a near constitutional crisis, and cast a shadow over the authority of Hong Kong's Court of Final Appeal as the final arbiter of human rights and the rule of law in Hong Kong. Most recently, in September 2002, the government, acting under Article 23 of the Basic Law, introduced vague and overbroad national security legislative proposals that, had they been enacted, would have had a very negative effect on human rights in Hong Kong.

But Human Rights Monitor's concerns are also based on the government's foot-dragging on electronic surveillance, as well as its recent decision to issue an executive order, without any input from the Legislative Council, and without even consulting with its own Executive Council, despite the Basic Law imperative that it should do so. The long period of inaction, coupled with the recent executive order, have given the impression that the government is less interested in its legal obligations and restrictions on its power under the Basic Law, and more interested in preserving the status quo of regulation of electronic surveillance, in which procedural requirements are minimal, and no outside oversight is allowed.

This briefing paper describes the current legal framework governing electronic surveillance in Hong Kong, as well as past attempts to address the problem and the constitutionality of the government's executive order. Although information is scarce, this paper attempts to describe, to the extent possible, the practice of covert surveillance in Hong Kong. Finally, this paper also looks at international law and comparative practice in order to make some recommendations on how the government should proceed with legislation to cover electronic surveillance.

[6] It is likely that the Government could have bought itself more time merely by signaling that it would legislate, and announcing a rough timetable for the introduction of legislation. Once the courts of Hong Kong were on notice that the government was working towards appropriate legislation, they would likely have given the government the benefit of the doubt and allowed the government to continue to engage in electronic surveillance until the legislation was introduced.

[7] Hong Kong Human Rights Monitor interview with Legislative Councillor, Hong Kong, October 2005.

n particular, the Hong Kong government should:

- Withdraw its August 2005 Executive Order and pledge to begin working with the Legislative Council immediately to come up with a proper alternative to the Order.

- Work directly with all parties in the Legislative Council to formulate a draft bill to cover covert surveillance. The legislation should ensure that all electronic surveillance is conducted only with judicial approval.

- New legislation should permit the authorization of covert surveillance only for the investigation of serious crimes, and only when the government has demonstrated that the surveillance will produce information of significant value to the investigation that could not be obtained by other, less intrusive means. Balancing tests, like those found in the August 2005 Executive Order, should not be used. [8]

- Pledge not to create a separate system for the review and approval of electronic surveillance on individuals suspected of engaging in activity that is a threat to state security. Instead, the government should require judicial authorization of all electronic surveillance, regardless of the type of activity being investigated.

- Any legislation that empowers the government to engage in electronic surveillance for the purposes of protecting "public security" or "public safety" should have very clear definitions for such terms. In general, authorization of surveillance on "public security" grounds should be limited to the investigation of alleged or planned acts of espionage, sabotage, or politically-motivated violence.

- Bring into force the Interception of Communications Ordinance, and work with LegCo to strengthen, through legislative amendment, its language on when wiretaps should be permitted. In particular, the government should seek to clarify the Ordinance's language on the use of wiretaps to protect the "security" of Hong Kong, to ensure that the wiretapping power is not used to engage in surveillance of peaceful political opponents of the government's policies.

- Work with LegCo to create a system of annual review and disclosure of the frequency of use of electronic surveillance. The goal should be to disclose, to the maximum extent possible, information on the government's use of electronic surveillance.

II. The right to privacy in international and comparative law

The Chief Executive has chosen to intercede in an area that is central to the liberty and security of the people of Hong Kong: the right to freedom and privacy of communications, protected by Article 30 of the Basic Law.

[8] Law Enforcement (Covert Surveillance Procedures) Order, Part 1, Section 3.

Article 30 of the Basic Law reads as follows:

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

The right to privacy is also protected in Hong Kong by Article 14 of the Bill of Rights Ordinance (BORO). Both Article 30 of the Basic Law and Article 14 of the BORO are similar in language, content, and scope to Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which reads as follows:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.
>
> Everyone has the right to the protection of the law against such interference or attacks.[9]

Both instruments contain the same two central elements, that of a right to privacy, and of the right to protection of that right by law.

The right to privacy is implicated in a broad range of issues, including the right against unwanted intrusion by the media or by private citizens,[10] the right to have one's personal data protected from misuse or abuse, and, in the modern context, the right to engage in private homosexual conduct[11] and the right to make one's own reproductive choices, free from government interference.[12]

At the very heart of the right to privacy is the right to be protected from unwanted intrusion into one's private thoughts, conversations, and actions. The Australian Law Reform Commission pointed out the risks to privacy posed by electronic surveillance in no uncertain terms:

> … the intentional surveillance of an individual's activities or conversations can have a corrosive effect on his sense of privacy and is

[9] The ICCPR is applicable to Hong Kong; under Article 39 of the Basic Law, both the ICCPR and the ICESCR remain fully in force in Hong Kong law, subject to the relevant reservations. The Bill of Rights Ordinance (BORO) also reinforces the applicability of the ICCPR to Hong Kong.

[10] For one of the earliest and most influential discussions of the right to privacy in the common law, see Warren and Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193-219, December 15, 1890.

11 See *Lawrence v. Texas*, 539 US 558 (2003).

12 See *Roe v. Wade*, 410 US 113 (1973).

> generally considered as a serious affront to the integrity of the individual subjected to this practice.[13]

Over the past several decades, technological advances have dramatically increased the ability of both governments and private individuals to spy on unsuspecting individuals.[14] Without the proper legal framework to prevent the misuse of this technology, no one can be sure that they are safe from prying eyes and electronic ears.

Because of its intensely intrusive nature, electronic surveillance is an enormous power that must be used judiciously – and, if possible, sparingly – by the government. As one jurist put it, "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance."[15]

Given the potential for very serious negative impact on individual privacy, most countries have created laws that closely regulate the use of electronic surveillance technology by various authorities, and most democratic countries require that law enforcement agencies first seek judicial authorization before engaging in electronic surveillance, just as they would when seeking to engage in a physical search.[16]

In the United States, the need for a judicial warrant was recognized in the 1967 *Katz* case. Abandoning once and for all its decision in the 1928 *Olmstead* case,[17] the Court declared that wiretaps are in fact a type of "search," and as such, can only be conducted pursuant to a judicial warrant. In support of its decision, the Court noted that

> the Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .' 'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment…[18]

After *Katz*, the same strictures that had long applied to police searches of an individual's home or office were applied to the use of wiretaps or other forms of electronic surveillance: law enforcement officials had to apply for judicially-issued warrants before engaging in any form of electronic surveillance.[19]

---

[13] Australian Law Reform Commission, *Discussion Paper on Privacy and Intrusions*, in *Covert Surveillance in Commonwealth Administration: Guidelines*, February 1992, p. 2.
[14] According to one expert commentator, "(b)ugging equipment has become much more sophisticated in the last twenty years, with the result that it is now very powerful, readily concealable, and relatively cheap." Fenwick, *Civil Liberties and Human Rights*, 3rd Edition, Cavendish Publishing Ltd., London, 2002, p. 689.
[15] Duarte (1990) 65 DLR (4th) 240.
[16] Privacy International, *Threats to Privacy*, "Legal Protections and Human Rights," November 12, 2004.
[17] *Olmstead v. United States*, 277 U.S. 438.
[18] *Katz v. United States*, 389 U.S. 347 (1967), 357.
[19] 389 U.S. 347, 358-9.

A handful of countries, the United Kingdom among them, rather than relying on judicial warrants, instead set up special commissions to oversee and authorize surveillance by the government.[20]

A legal framework that requires judicial or other outside oversight, while central to a regulatory regime, is not in itself sufficient. The law should also make clear the conditions under which electronic surveillance can be used, and give guidance to the authorizing authority as to what level of evidence is needed to permit electronic surveillance. Without such guidance, the requirement for judicial authorization can become a triumph of form over substance.

In other words, the police cannot ask for broad authority, and judges cannot be empowered to issue a blank cheque. Instead, the law has to be sufficiently clear as to when the surveillance power can be granted, under what specific circumstances, and when and how that grant of power must be renewed. According to the European Court of Human Rights:

> … the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence….[21]

In the United Kingdom, for example, certain forms of covert surveillance can only be authorized to investigate a "serious crime," and if the surveillance will likely be of "substantial value" and that "the objectives of the [surveillance] cannot reasonably be achieved by other means."[22]

The definition of what constitutes a "serious crime" is handled differently in various jurisdictions; a number of national governments have used the length of imprisonment for the commission of the crime being investigated as a yardstick for seriousness. In the United Kingdom, any crime that carries a penalty of three years or more in prison can be considered a serious offense. Crimes that involve the use of violence, results in

---

[20] The UK system does allow for authorization of surveillance by a senior police officer in certain situations, but even in those situations, the relevant commissioner must be notified of the authorization as soon as it is given. Prior outside approval is required when the authorities wish to engage in surveillance of a "dwelling, hotel bedroom, or office premises." Fenwick, *Civil Liberties and Human Rights*, 3rd Edition, Cavendish Publishing Ltd., London, 2002, p. 693. Some observers have expressed reservations about the effectiveness of the system, given the lack of outside oversight and prior approval required in certain situations. Hong Kong Human Rights Monitor believes that Hong Kong should adopt a system which, like the American framework, requires prior judicial approval under virtually all circumstances.

[21] *Malone v. United Kingdom*, (1984) 7 ECHR 14, paragraph 64.

[22] United Kingdom Police Act 1997, s. 93(2). For further discussion of the legal framework governing covert surveillance in the UK, see Cheney et al., *Criminal Justice and the Human Rights Act 1998*, Jordan Publishing, Bristol, UK, 2001, p. 95-105.

substantial financial gain, or is conducted by a large number of persons in pursuit of a common purpose also fall into the "serious crimes" category.[23]

In addition to authorizing electronic surveillance for the investigation of "serious crimes," many jurisdictions also authorize electronic surveillance on "national security" grounds. In order to avoid the risk that security be used as an excuse to engage in political surveillance, it is crucial that the term "security" be carefully, and narrowly, defined, so that it covers only acts that are a genuine threat to security.

In Australia, under the Australian Security Intelligence Organisation Act, "security" is defined as:

> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
> (i) espionage;
> (ii) sabotage;
> (iii) politically motivated violence;
> (iv) promotion of communal violence;
> (v) attacks on Australia's defence system; or
> (vi) acts of foreign interference;
> whether directed from, or committed within, Australia or not; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).[24]

Other jurisdictions have adopted similar definitions.

Hong Kong's status as a Special Administrative Region (SAR) means that it does not need to empower certain types of surveillance. In particular, provisions relating to communal violence, attacks on the defense system, and acts of foreign interference are not necessary in Hong Kong, as there is no history of communal violence in Hong Kong, and Hong Kong has no standing army of its own.

Hong Kong's British colonial past also inhibits the creation of narrowly-tailored law in this area. Because a number of legal terms, including treason and sedition, retain outdated colonial definitions and have yet to be reformed, the Hong Kong government should not authorize surveillance on these grounds. The collapse of the government's Article 23 proposals in September 2003 also played a key role. As it stands, Hong Kong law currently lacks clear and precise definitions for a number of "national security" crimes.

In the light of Hong Kong's recent controversies over national security-related legislation under Article 23 of the Basic Law, Human Rights Monitor urges that Hong Kong law

---

[23] Fenwick, *Civil Liberties and Human Rights*, 3rd Edition, Cavendish Publishing Ltd., London, 2002, p. 692. Police Act, s. 93(4).
[24] ASIO, section 4.

should not yet authorize any surveillance on the grounds of "national security" until the discussions on national security legislation under Article 23 are resumed. Once the government and the people of Hong Kong have had a chance to deal with the modernization of the law in this area, regulations governing surveillance can be easily amended in light of any new laws. Until that time, much of the government's surveillance needs can be met by provisions allowing for surveillance to investigate "serious crimes."

Many governments – the United States, the United Kingdom, Australia, and Canada among them – have also created legislative requirements for annual disclosure by the government of the extent of its use of electronic surveillance techniques.[25] Such annual disclosure requirements can protect against a sudden surge in usage by the government, and give the public some sense of the extent of government reliance on electronic surveillance as a means of protecting the safety and security of its citizens.

The right to privacy in Hong Kong

In many ways, the Hong Kong government, after an extremely late start, has been quite vigilant in protecting the privacy of Hong Kong citizens. The government has protected personal data from theft or abuse under the Personal Data (Privacy) Ordinance, and, in accordance with international guidelines, has appointed a privacy commissioner to oversee the protection of individual privacy in Hong Kong.[26]

There have been occasional departures from this improved record: in February 1997, the central government in Beijing announced that, among other laws, section 3(2) of the Personal Data (Privacy) Ordinance would be invalidated after the July 1, 1997, handover.[27] Section 3(2) integrated the protections of the ICCPR and the Bill of Rights Ordinance into the Personal Data (Privacy) Ordinance.

In 1998, in perhaps the only example of government refusal to enforce the Personal Data (Privacy) Ordinance, the SAR government declined to prosecute the Hong Kong office of the New China News Agency (known by its Chinese name, *Xinhua*) for failing to meet the statutory deadline for disclosing to pro-democratic legislator Emily Lau the extent and details of personal information it had about her in its files. In response to a 1996 request by Ms. Lau, Xinhua responded that it had no information on her, a claim that most observers viewed with some skepticism, given Xinhua's role as the Chinese government's *de facto* representative office in Hong Kong before the 1997 handover. Its response came much later than the 40-day deadline required by the statute, yet the government declined to prosecute, citing insufficient evidence and vague "public interest

[25] Privacy International, *Threats to Privacy*, "Legal Protections and Human Rights," November 12, 2004.
[26] Personal Data (Privacy) Ordinance, cap. 486, s. 5.
[27] Decision of the Standing Committee of the National People's Congress Regarding the Treatment of the Existing Hong Kong Laws According to Article 160 of the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China, 23 February, 1997. In particular, the Decision invalidated the "[p]rovisions concerning the [Bill of Rights] Ordinance's overriding position in section 3(2), of the Personal Data (Privacy) Ordinance (Chapter 486, Laws of Hong Kong)."

concerns."[28] The decision not to prosecute left the impression that, less than a year after the handover, the SAR government was reluctant to take on entities connected to Beijing for violations of the law.

These important exceptions aside, the government has, by and large, upheld data privacy laws, and has continued to protect the citizens of Hong Kong from misuse or abuse of their personal information by private companies or government bureaus.

But in other key areas in which its own police power comes up against the individual right to privacy, the government, both before and after the 1997 handover, has performed much less admirably. The Hong Kong colonial government, following in the footsteps of British government itself, failed to enact basic safeguards against government abuse of its power to tap phones and intercept written communications, despite the clear threat that such intercepts can pose to individual privacy. And it failed to enact any laws whatsoever constraining the power of the government to engage in covert surveillance of its own citizens. The post-1997 Special Administrative Region (SAR) government followed suit: satisfied with the status quo, it, too, did nothing.

III. Electronic surveillance in Hong Kong: a murky history

Very little is known about the extent of the government's use of covert surveillance, either during the British colonial era or since the 1997 handover. In 1999, a Hong Kong newspaper obtained leaked statistics on government use of phone taps, which indicated that government wiretaps ranged between 50 and 100 at any given time, with the majority of those being issued by the ICAC.[29] No similar statistics were disclosed on the government's use of covert surveillance.

Even in the absence of hard data, some of the central targets of electronic surveillance by Hong Kong authorities over the years are known, and their identity comes as no surprise: the primary targets of surveillance were, early on, Communists, and to a lesser extent, their KMT rivals. When the government got serious about combating corruption in the 1970s, the Hong Kong police, other government officials, and private businessmen engaged in allegedly corrupt activity became a key target. Finally, in the 1980s and 1990s, Hong Kong's early pro-democratic activists found themselves on the government's surveillance list. The extent of surveillance of pro-democratic activists by the SAR government since 1997 is not known, but some in the democratic camp have publicly complained of their belief that they are being targeted by unlawful – or at least unregulated – government surveillance.

---

[28] David Newman and Alvin Rabushka, *Hong Kong Under Chinese Rule: the first year*, Hoover Institution, Eassays in Public Policy, section 2.

[29] Michael Chugani, "Government loath to surrender its powers to the courts," Hong Kong *Standard*, September 29, 1999. The newspaper reported that, since the 1997 handover, the number of wiretaps had "climbed higher," but the paper could offer no information as to whether the new government had expanded the scope of surveillance to cover pro-democracy politicians and civil society groups.

The government organ responsible for surveillance of political actors in British Hong Kong was the Special Branch of the Hong Kong police force, which functioned as the British Colonial government's quasi-intelligence agency. Its original name was a clear marker of its primary target: founded in 1930, the Anti-Communist Squad renamed itself "Special Branch" (*Zhengzhi Bu*, or Political Bureau, in Chinese) a few years later.[30] Despite the name change, the Special Branch remained focused on Communist activity in Hong Kong:

> As a colonial force, the Hong Kong police had traditionally been organized as a paramilitary force, with much greater emphasis laid on maintaining internal security than in any police force in, say, the United Kingdom. This role took on new importance in post-war Hong Kong as the Chinese Civil War between the Communist Party and the Kuomintang entered a period of stalemate in 1950, and Hong Kong became their most important place for intelligence or covert operations against each other. Two separate, though related, internal security tasks thus confronted the Hong Kong police. The first such task was to monitor and counter what one could loosely describe as 'cloak and dagger' activities of the two Chinese protagonists. *This was the responsibility of the Special Branch. … The second internal security task was to maintain stability and good order, either by pre-empting major disturbances, politically inspired or not, or by containing and suppressing them efficiently once they started*.[31]

The tools at the Special Branch's disposal were many and varied, and included the ability to deregister organizations that it believed had been successfully infiltrated by the Communists.[32] Electronic surveillance was also a key part of the Special Branch's arsenal. According to one senior Communist Party member who had worked in Hong Kong, bugging was a fact of life for known senior CP agitators:

> In the anti-British, anti-repression struggle [referring here to the 1967 riots], much of the party organization had been exposed, and was destroyed. Yet we did not know whose identity had been exposed, and whose had not. … (T)he local party was divided into two lines, the workers line and the schools line, and the leaders of both lines had their homes bugged by the Hong Kong British authorities.[33]

---

[30] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong," *Hong Kong Law Journal*, vol. 33, part 1, 2003, p. 203.
[31] Steve Tsang, ed., *A Documentary History of Hong Kong, Government and Politics*, Hong Kong University Press, 1995, pp. 173-4. Emphasis added.
[32] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong," *Hong Kong Law Journal*, vol. 33, part 1, 2003, p. 205.
[33] Tsang, ed., *A Documentary History of Hong Kong, Government and Politics*, Hong Kong University Press, 1995, p. 299.

Electronic surveillance was not limited to members of the Party in Hong Kong: various pro-China organizations, not formally a part of the Party structure in Hong Kong, were also kept under surveillance.[34]

While continuing to keep an eye on Communist and other leftist political activity, the government was forced to deal with a much more long-standing problem: that of rampant corruption. Corruption, particularly in the police force, had been a part of Hong Kong almost from its inception as a colony in the late 19th century. By the mid-1960s, the problem was perceived as being almost totally out of control. The situation was so bad that it was feared that there was nothing that could be done:

> … a great deal of crime was generated by the police force itself. Desk sergeants in local police stations became millionaires as they controlled the distribution of bribes and the allocation of protection rackets organized by the police. The force was so riddled with corruption that successive post-war colonial governments avoided confronting the issue, fearing that it would lead to a total breakdown of law and order.[35]

The ICAC was created in 1974 by the then British Governor Lord Murray MacLehose to combat the corruption plague, and it was given wide-ranging powers, described as almost "draconian" by one expert observer, to do so. These powers included the authority to engage in electronic surveillance.

Although the process took several years, and the government, facing a near-riot on the part of its own police force over the ICAC's aggressive investigations, had to issue an amnesty for all but the most serious cases, the ICAC did manage to fulfill its mandate to "break the back of corruption" in Hong Kong. It continues to perform that vital task today.

But its success has come at a price: the aggressive tactics that came to light in the April and July 2005 court cases were apparently by no means unusual. In 1993, former ICAC senior official Alex Tsui testified before LegCo that the ICAC had taken over some of the Special Branch's political surveillance duties, and that the Commission had tapped the phones of several senior government officials, including former Executive Council member Rita Fan.[36]

According to several individuals with firsthand knowledge of Hong Kong's legal community, many Hong Kong barristers who take corruption cases refuse to discuss legal strategy over the phone, and some are even unwilling to talk to their clients about particularly sensitive issues in their own offices.[37]

---

[34] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong," *Hong Kong Law Journal*, vol. 33, part 1, 2003, p. 209.
[35] Steve Vines, *Hong Kong: China's New Colony*, London: Aurum Press, 1998, p. 245.
[36] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong," Hong Kong Law Journal, vol. 33, part 1, 2003, p. 220.
[37] Hong Kong Human Rights Monitor interviews, Hong Kong, October 2005.

In the absence of any public disclosure or description of the ICAC's use of its extensive electronic surveillance powers, no evidence exists, beyond the facts of the July 2005 *Shum Chiu* case, [38] to confirm the fears of those barristers who take extra precautions. Yet the *Shum Chiu* case took few lawyers in Hong Kong by surprise: as one Hong Kong lawyer who takes some precautions when communicating with clients being investigated by ICAC pointed out, it seems unlikely that that was the first or only time that the ICAC has engaged in such behavior.[39]

It is possible that what happened in the *Shum Chiu* case is in fact representative of the way in which the ICAC and other government agencies use their almost completely unfettered power to engage in electronic surveillance: they may use it to make sure that, when a case that they are investigating goes to court, they already know what the other side plans to do. Thus forewarned, they are much more certain of a successful prosecution.

"Because there is no legislation, there is concern that law enforcement agencies will act in a way that will maximize their advantage when it comes to litigation," one lawyer said. "Frankly, Hong Kong is in the dark ages when it comes to this."[40]

Political surveillance: 1980s-present

The most troubling area of covert surveillance by the Hong Kong government is that area which is the least well-known, that of "political" surveillance. Political surveillance refers to surveillance of individuals who are either engaged in peaceful opposition political activity or those who the government believes may be engaged in political activity that is in fact illegal, and the surveillance of whom is justified on national security grounds.

Both the British colonial government and the current SAR government have engaged in political surveillance, but the extent of the practice, either before or after 1997, is not known.

One of the few known examples of political surveillance by the British colonial government to come to light was the monitoring of one of Hong Kong's earliest civil society groups, the Hong Kong Observers, in the 1980s.[41] Members of the group included longtime journalist and commentator Frank Ching and later LegCo member and current head of the group Civic Exchange, Christine Loh. The group's activities were limited to peaceful public advocacy and monitoring of political and legal reform in Hong Kong, yet the British colonial government decided to keep a close eye on some of its members.

The monitoring of the Observers was carried out by a secret government committee, formed especially for the purpose of monitoring civil society groups, called the Standing

[38] *HKSAR v. Shum Chiu and Others*, Criminal Case no. DCCC 687 of 2004, 5 July 2005.
[39] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.
[40] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.
[41] Hong Kong Human Rights Monitor, *Hong Kong: NGOs step into the unknown facing repressive laws*, September 1997, p. 1.

Committee on Pressure Groups.[42] The surveillance activities of the Standing Committee were not limited to the Observers; other social groups were also apparently monitored, including the Society for Community Organization and the Heritage Society.

Despite the severe infringement on individual rights that such surveillance entailed, the government carried out the monitoring in secret, and its targets found out only by chance. According to then-Observer member Anna Wu:

> At the time, we had no idea that there was a secret committee within the government that was keeping us under surveillance. We only found out because these secret reports were leaked to the British press. To date, they have not been released by the government. For all we know, these reports are still in our personal dossiers, read by civil servants who may still believe their contents. I asked the Governor for permission to have access to dossiers kept on me by the government, but Mr. Patten has not yet given me a positive response.[43]

After 1997, some pro-democratic activists and legislators, including Legislative Councillor Leung Kwok-hung, known as "Long Hair" and former Legislative Councillor Szeto Wah, have stated that they believe that they are subject to wiretapping and other forms of electronic surveillance, but they could only cite anecdotal evidence in support of their claim. No concrete proof of such activity has yet emerged, but in the absence of any government transparency regarding its use of covert surveillance, suspicions remain.

In at least one case, the government's perceived need to engage in political surveillance took precedence over an ongoing criminal investigation. According to an individual approached by the police officer himself, a member of the Hong Kong police intelligence surveillance unit was taken off a drug surveillance case to monitor a "second-tier activist" for a brief period.[44] This police officer was upset by this reprioritization of resources, and regarded the surveillance of the political activist as little more than a waste of time.

Many pro-democratic activists also fear that the government may have stepped up its political surveillance in the wake of the massive July 1, 2003 protests in Hong Kong. Beijing was deeply unhappy about being caught off-guard by the protests and, according to some observers, informed the SAR government of their displeasure and the need to take action:

> They came to conclusion that Ms. Ip was not keeping them informed. We must have a Special Branch again, otherwise we won't know what's going on, [was the government's thinking]. They think it's horrible that they don't have an apparatus like the Special Branch to know what's going on.

---

[42] Ibid.
[43] Anna Wu, "Human Rights: Rumor Campaigns, Surveillance and Dirty Tricks and the Need for a Human Rights Commission," *Hong Kong's Bill of Rights: 1991-1994 and Beyond*, Proceedings of a Seminar Organized by the Faculty of Law, University of Hong Kong, 18 June 1994, p. 75.
[44] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.

> How can a group like Civil Human Rights Front have the power to do this [referring to the staging of the massive July 1, 2003, demonstration] and we don't know about it?[45]

The government's veil of secrecy on political surveillance has been repeatedly challenged by pro-democratic members of LegCo, but they have yet to force any significant disclosure by the government of their activities in this area. Yet Hong Kong's history of politically-motivated surveillance of prominent opposition activists engaged in peaceful activity indicates the need for strong protections against abuse.[46]

IV. Hong Kong law on electronic surveillance and attempts at reform

As a British colony, Hong Kong for much of its history did not enjoy particularly strong basic rights protections. When it came to electronic surveillance, Hong Kong residents were in the same boat as their British colonial rulers: both the United Kingdom and Hong Kong lacked any significant safeguards against the unfettered use of wiretapping or covert surveillance by the government.

The same lack of sufficiently protective legislation remains in Hong Kong today. Wiretapping is still covered by section 33 of the Telecommunications Ordinance, which specifies that the Chief Executive can order a wiretap merely if he believes doing so is in the "public interest," an extremely broad term that is left undefined. No outside approval, either in the form of a judicial warrant or otherwise, is needed.

The statute, which uses virtually identical language to the corresponding regulation in the UK since replaced, is breathtakingly broad:

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

---

[45] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.

[46] Some Hong Kong legislators have speculated that political surveillance in Hong Kong is funded by a line in the Hong Kong police budget, which is referred to as "rewards and special services." Despite repeated requests over a period of several years for more information on how these funds are used, the government has yet to provide any accounting, and has deflected all questions on the matter as inappropriate, given the "confidential" nature of the expenditures. The budget line is not insignificant: it runs to more than HKD$100,000,000 (roughly USD$13 million) per annum, about 1% of the overall police budget. Legislative Council, Official Record of Proceedings, 31 March 1999.

Because the government does not publicly disclose any statistics on the frequency of use of wiretaps, it is impossible to know to what extent, if at all, the law has been abused.[47]

The public interest standard articulated in Section 33 is perhaps the lowest possible standard that could be put forward. There is no requirement that the government believe that a crime, or, even more narrowly, a serious crime, is being, or is about to be, committed. Nor is there any requirement that the government articulate its reasons for believing that the individuals it seeks to monitor are in fact engaged in criminal activity, or otherwise produce any evidence to substantiate its concerns.[48] Finally, there is no requirement that the government demonstrate that there are no other, less intrusive means of acquiring the information sought.

Instead, the government need only conclude that it is in the public interest for electronic surveillance to take place. No further definition of "public interest" is given, and no other restrictions are placed on the government's ability to engage in interception of communications. In essence, it is left entirely up to the government to decide, without outside review, how to strike the balance between the need for proper powers to ensure the safety and security of Hong Kong and the individual right to be free from unwanted government intrusion. It is unlikely that this law, with its vague and broad grant of power to the Chief Executive, would be considered to be in accordance with Article 30 of the Basic Law.

As weak as the wiretapping provision is, it is still better than the law on covert surveillance, which is, in essence, no law at all. Despite the intense intrusiveness of covert surveillance, the British colonial government left the operation of and limitations on covert surveillance to the administrative regulations, or Standing Orders, of the various departments that would carry out the activity. For its part, the SAR government did nothing to fix the problem.

The problems of regulating the issue through Standing Orders are many: first, Standing Orders are generally internal documents, and, unlike laws, are not subject to public scrutiny.[49] Secondly, such standing orders are difficult for LegCo to fix: under the Basic Law, LegCo members cannot introduce bills that affect "government policies" without the written consent of the Chief Executive.[50] It is almost certain that the government would not permit the introduction of such a bill. Finally, such Standing Orders fail to

[47] H. L. Fu and Richard Cullen, "Political Policing in Hong Kong," *Hong Kong Law Journal*, vol. 33, part 1, 2003, p. 219.
[48] Although Section 33 creates no legal requirement that the government do so, the government has in the past claimed that it limits the use of wiretaps to "cases involving the prevention or detection of serious crime, including corruption, or in the interests of the security of Hong Kong." Hong Kong Hansard, 11 November 1992, p. 634.
[49] *HKSAR v. Li Man Tak and Others*, paragraph 21.
[50] Article 74 of the Basic Law reads: "Members of the Legislative Council of the Hong Kong Special Administrative Region may introduce bills in accordance with the provisions of this Law and legal procedures. Bills which do not relate to public expenditure or political structure or the operation of the government may be introduced individually or jointly by members of the Council. The written consent of the Chief Executive shall be required before bills relating to government polices are introduced."

provide any significant safeguards against the abuse of covert surveillance power. Most crucially, the process set up by such Orders does not provide for outside oversight of the use of covert surveillance by the government.

In essence, the framework for covert surveillance in Hong Kong was the same as that of the United Kingdom before the UK began legislating in this area in the late 1990s. Before the passage of the UK Police Act 1997, which provided for the first time in British history a statutory basis for covert surveillance, such action was covered by Home Office Guidelines, issued in 1984. The Guidelines suffered from the same weaknesses as the Standing Orders: the Guidelines were not generally publicly available,[51] and they did not provide for any mechanism for outside review of decisions to engage in covert surveillance.[52]

Some momentum was generated for reform in Hong Kong by the 1984 European Court of Human Rights decision in the *Malone* case. After the *Malone* decision, the Hong Kong government was advised that it too was vulnerable to a legal challenge along the lines of the case in Strasbourg.[53] The Hong Kong colonial government's legal obligation to act was also strengthened by the passage of the Bill of Rights Ordinance (BORO) in 1991. Spurred in part by the 1989 killings of innocent protestors in and around Tiananmen Square, and the imminence of the return of sovereignty over Hong Kong to the Chinese government, the Hong Kong government created the Bill of Rights Ordinance (BORO), the colony's first Bill of Rights in nearly a century of British rule.[54]

In essence, the BORO was Hong Kong's legislative response to Article 2 of the ICCPR: it implemented into domestic law the provisions of the ICCPR.[55] Under the Bill of Rights Ordinance, the government was obligated to examine all of its laws to ensure that they

---

[51] *Khan v. United Kingdom*, [2000] ECHR 194, 12 May 2000, paragraph 23.

[52] The ECHR court in the *Khan* case summarized the authorization process under the Guidelines as follows: In each case, the authorising officer should satisfy himself that the following criteria are met: (a) the investigation concerns serious crime; (b) normal methods of investigation must have been tried and failed, or must from the nature of things, be unlikely to succeed if tried; (c) there must be good reason to think that the use of the equipment would be likely to lead to an arrest and a conviction, or where appropriate, to the prevention of acts of terrorism; (d) the use of equipment must be operationally feasible. The authorising officer should also satisfy himself that the degree of intrusion into the privacy of those affected by the surveillance is commensurate with the seriousness of the offence.

[53] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.

[54] National Democratic Institute, *The Promise of Democratization in Hong Kong, NDI Pre-election Report #1*, June 10, 1997, p. 9. The government had moved quickly: the Legislative Council had publicly called for a bill of rights for Hong Kong in April 1990; the entry into force of the BORO came just over a year later, in June 1991.

[55] Under Article 2 of the ICCPR, "each State Party… (shall) take the necessary steps, in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant." The BORO also made explicit its goal of bringing the protections of the ICCPR into force in domestic Hong Kong law. According to Article 2(3), all branches of government, "(i)n interpreting and applying this Ordinance, regard shall be had to the fact that the purpose of this Ordinance is to provide for the incorporation into the law of Hong Kong of provisions of the International Covenant on Civil and Political Rights as applied to Hong Kong…."

were in compliance with stringent civil and political rights protections.[56] Many commentators accused the outgoing British colonial administration of base hypocrisy: the colonial government was a latecomer to the issue of human rights protections for the people of Hong Kong, taking an interest only on the eve of its departure.

This critique was not without merit, but it failed to take into account that many of the prime movers behind the creation of the BORO were local Hong Kong legislators, lawyers, and activists, all of whom would be staying on in Hong Kong after the return of sovereignty was complete and the colonial government had passed into history. Far from trying to protect Britain's historical legacy, these men and women were trying to build a bulwark against future attacks on their rights by a government that did not yet exist.

In the years between 1991 and the 1997 transfer of sovereignty, the Hong Kong government conducted a thorough review of its laws, and engaged in a number of far-reaching reforms. Many of the regulations relating to the basic freedoms of expression, association, and assembly were woefully antiquated, in many cases reflecting a pre-WWII colonial mindset. But the passage of the BORO gave all three branches of government a chance to examine all of these issues anew:

> The coming of the Bill of Rights brought with it a wide-ranging policy review in many areas, and some of the detritus of legal history was swept away as the result of judicial pronouncements of inconsistency, and subsequent legislative reform. The Bill of Rights also gave stimulus to the enactment of detailed legislation in other fields… The courts of Hong Kong have become reasonably familiar with relevant international materials, with judgments regularly drawing on the jurisprudence of the United Nations treaty bodies (in particular the Human Rights Committee) and, more extensively, the jurisprudence of the European Convention on Human Rights, as well as human rights and constitutional law from many national courts.[57]

Although the BORO had a significant impact on many areas of Hong Kong's criminal law and criminal procedure including bail regulations, protection of the right to presumption of innocence, and the right to a speedy trial, the need to reform electronic surveillance laws was more or less ignored by the government in the first few years after the passage of the BORO.[58]

---

[56] Hong Kong BORO, Arts. 3, 4, 6.

[57] Andrew Byrnes, *Jumpstarting the Hong Kong Bill of Rights in its Second Decade? The Relevance of International and Comparative Jurisprudence.* Although the Chinese government had for years railed against the evils of Western imperialism, it nonetheless protested bitterly over some of the changes enacted in the last years of British rule, promising to turn them aside when it took over. Within months of coming into power, the newly-formed Special Administrative Region (SAR) government did just that.

[58] It is possible that the government did improve its practice as regards covert surveillance, although there is no evidence that it did so. The government did say that, in light of the Bill of Rights, it was paying more attention to "the appropriate exercise of police powers and the avoidance of anything that can be characterized as an abuse of process," even in the absence of a court decision or new legislation specifically mandating that they do so. See SR Bailey, "Criminal Law and Procedure," *Hong Kong's Bill of Rights:*

Perhaps because there already was a law on the books governing interception of communications, potential reforms in that area received more attention than covert surveillance.[59] As early as 1992, the Secretary said that the government was looking at the question of whether or not the laws on interception of communications would have to be liberalized to conform to the Hong Kong Bill of Rights, in particular Article 14,[60] which protects the right to privacy:

> I can confirm that we are looking at our legislation to see if it is in need of modernization in the light of the introduction of the Bill of Rights, and a review is now underway. In this review we will take carefully into account the recommendations of the Law Reform Commission, which is presently examining existing Hong Kong laws affecting privacy, including the interception of communications.[61]

Despite these words, and other assurances by the colonial government that it was indeed "reviewing" the matter, the government did nothing, and the law remained unchanged. No action was taken until several years later, just months before the July 1, 1997 return of sovereignty to mainland China.

The final hours: Pre-handover attempts at legislation

In 1996, the Law Reform Commission of Hong Kong suggested that Hong Kong law be amended to ensure that all electronic surveillance be carried out under a judicially-issued warrant:

> We consider that the additional independence afforded by a judicial determination is necessary in Hong Kong. … *The advantage of having a judge scrutinise all applications is that it ensures that those applying for the warrant will have to think the matter through. This diminishes the prospect of abuse of power. It is also reassuring to the public.* Restricting the power to the High Court should also make for greater consistency of approach. Accordingly, we recommend that all applications for warrants for surveillance or interception should be made to the High Court.[62]

1991-1994 and Beyond, p. pp. 42-3. Whether or not they applied this greater scrutiny to their covert surveillance tactics, even temporarily, is not known.

[59] Also, the case that forced the British government to liberalize its covert surveillance regulations, *Khan v. United Kingdom*, was not decided until 1997.

[60] Article 14 of the BORO duplicates the language of Article 17 of the ICCPR; given the tie-in to Article 17, and the ways in which the Bill of Rights Ordinance as a whole links itself to the ICCPR, the jurisprudence of the UN Human Rights Committee on the issue of privacy in general and electronic surveillance in particular should be considered highly persuasive to the courts of Hong Kong. See, e.g., BORO, Arts. 2(3), 4.

[61] Hong Kong Hansard, 11 November 1992, p. 40.

[62] Law Commission of Hong Kong , Privacy Sub-Committee, *Privacy: Regulating Surveillance and the Interception of Communications*, December 1996, paragraph 6.18. Emphasis added.

After the release of the 1996 Commission study, the government promised to take action. But by early 1997, with just a few months to go before the handover, the government had yet to produce a document.

Then-Deputy Secretary for Security Carrie Yau stressed to a reporter that quality could not be sacrificed in order to meet the deadline. "We hope in the near future we can complete the drafting work – we are very active in doing this," Ms. Yau said.[63]

Finally, on February 29, 1997, the government issued a consultation paper, with a White Bill, on the Interception of Communications Bill, and called for public consultation until April 4. The government draft, though by no means perfect, was nonetheless a strong one: it included many of the protections suggested by the Law Commission, and also added some additional safeguards not included in the Law Commission report.[64] It did not, however, cover covert surveillance.

After the end of the consultation period, the government expressed doubts that the legislation could be readied in time. In a LegCo committee meeting on April 11, 1997, Deputy Secretary Yau told LegCo members that the government was still not yet ready to table a bill.[65]

The repeated government delays met with strong criticism from several legislators. Then-LegCo security panel Chairman James To threatened to introduce a motion criticizing the outdated legislative framework. LegCo member Emily Lau also called for action, pointing out that the wiretapping bill is a "sensitive issue," and noting that Governor Chris Patten had promised to deal with it.

Not all parties saw the necessity of rushing to pass a bill. "Of course, every person has their own privacy," said Ip Kwok-him, of the Democratic Alliance for the Betterment of Hong Kong (DAB). "But LegCo does not have much time left and it may be more appropriate if we discuss the bill after the handover."[66]

A month later, LegCo was still waiting for the government to send over a document. On May 9, the Security Bureau announced that there would be further delay, due to "technical and policy problems" raised during the consultation period.[67] The government was also concerned that it did not have the votes necessary to secure passage of the bill. Within weeks, the government, apparently believing that it had run out of time, dropped the bill entirely.

After the government finally declined to issue its bill, LegCo took matters into its own hands. With time running out before the handover, Legislative Councillor James To submitted a member's bill to regulate interception of communications.

---

[63] James Kelly, "Phone-tap bill could miss the last call," Hong Kong *iMail*, 19 February 1997.
[64] "Tapping Out of Time?," *South China Morning Post*, 1 March 1997.
[65] Genevieve Ku, "Tapping Indecision Bugs," *South China Morning Post*, 12 April 1997.
[66] Ibid.
[67] Genevieve Ku, "Patten accused over phone-tap bill delay," *South China Morning Post*, 10 May 1997.

Although he had initially included a provision covering covert surveillance, the time pressure associated with getting a bill through the LegCo before July 1, 1997, combined with the relative newness of the issue for many of his colleagues, led him to withdraw that provision. "If I could not get it passed and signed by the government, then there would be nothing, just a historical record," said To.[68]

"I started counting votes, and I realized that once I put more things in, then I would have to explain more about it," To said. "So I took [the provision on covert surveillance] out, in order to have at least something passed."[69]

The bill, the Interception of Communications Bill 1997, was the last bill passed by LegCo, on June 29th, 1997.

Though the new law did not cover covert surveillance, it was a significant improvement over Section 33 of the Telecommunications Ordinance. Under the new Interception of Communications Ordinance, electronic surveillance could only be carried out under a high court order.[70] The new ordinance also replaced the vague and expansive "public interest" rationale of the Telecommunications Ordinance with a requirement that surveillance warrants could only be used to investigate a "serious crime," or "in the interest of the security of Hong Kong."[71]

The colonial government expressed reservations about the bill, but outgoing British colonial governor Chris Patten signed the bill into law before the July 1 deadline.

Despite the improvements, the law never came into force. The law was to take effect upon the authorization of the Chief Executive – the SAR's replacement for the governor of Hong Kong – which was not forthcoming. During his more than seven years in office, the first post-handover Chief Executive of the SAR, Tung Chee-hwa, failed to bring the law into force.[72] His replacement, Donald Tsang, also did nothing during his several months in office before the April 2005 court case brought the issue once again into public view.

---

[68] Hong Kong Human Rights Monitor interview with James To, October 5, 2005.
[69] Hong Kong Human Rights Monitor interview with James To, October 5, 2005.
[70] Interception of Communications Ordinance, Cap 532, Section 4, Part III, clause (1).
[71] Interception of Communications Ordinance, Cap 532, Section 4, Part III, clause (2). Also, under clause (3), a judge had to be convinced that:
(a) there are reasonable grounds to believe that an offence is being committed, has been committed or is about to be committed;
(b) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought;
(c) all other methods of investigation have been tried and have failed, or are unlikely to succeed; and
(d) there is good reason to believe that the interception sought will result in a conviction.
[72] The failure to bring the law into force may itself be a violation of the Basic Law: under Article 64 of the Basic Law, the Chief Executive is required to "implement laws passed by the Council and already in force."

V. Reviving the discussion: the push from the courts

Despite periodic queries from individual LegCo members about the status of the law, the issue was effectively dead: restrictions on individual legislative councillors' ability to introduce legislation[73] meant that they could only plead with the government to take action. As long as the issue was kept out of the courts, the government could continue to sit on its hands. For almost eight years, the government managed to do nothing, despite the clear obligation under international law and its own domestic human rights instruments that it take action and legislate.

The April 2005 Li Man-tak case

As noted above, the case that brought the issue once again to the fore and forced the government's hand was the ruling in a *voir dire* application of District Court Judge Sweeney, issued on April 22, 2005.[74] The ruling concerned the admissibility of various recordings made by the Hong Kong Independent Commission Against Corruption (ICAC), a well-respected government agency that was investigating alleged conspiracy and bribery charges against a group of Hong Kong businessmen.

In the course of the investigation, the ICAC bugged two separate restaurants used by the defendants on two different occasions, apparently to discuss aspects of their alleged criminal conspiracy.

In his decision, the judge examined the current procedure – covered by internal ICAC "standing orders" – to see if it was in accordance with Article 30 of the Basic Law. The ICAC procedure, presumably typical of Hong Kong's law enforcement agencies in general, was not particularly onerous: under the standing orders, the investigator wishing to install a bugging device had to apply in writing to a sufficiently senior officer within the ICAC, who "considers such intelligence information and submitted grounds before deciding whether or not to authorize the installation of bugging devices."[75] He or she would then issue an authorization or refusal in writing to the officer.

The application and approval procedure was closed to the public, and completely contained within the ICAC itself. There was no requirement for judicial approval, and the decision was non-reviewable. No provisions were made for remedies or even disclosure in cases in which the authorities had abused their power to engage in surveillance. Even the minimum due process requirements called for under the ICAC standing orders were not met in the *Li Man-tak* case, as the officers involved in the execution of the covert surveillance did not create a written record of the request and its approval.[76]

[73] The restriction was introduced by Article 74 of the Basic Law, which requires that "(t)he written consent of the Chief Executive shall be required before bills relating to government policies are introduced."
[74] *HKSAR v. Li Man Tak and Others*, Criminal Case No. 689 of 2004, 22 April 2005, [2005] HKEC 1308.
[75] Ibid., paragraph 19.
[76] Ibid., paragraph 21.

ICAC official Tony Lui described the process of approving the request by investigator Patrick Ho to engage in surveillance:

> After carefully analysing the intelligence information received, I was of the view that covertly tape recording the meeting was the only means by which the ICAC could obtain important evidence of this very serious corruption offence. I was conscious of the provision of Article 14 of the Hong Kong Bill of Rights Ordinance that no one shall be subjected to arbitrary or unlawful interference with his privacy and understood that by making covert tape recordings, individual privacy, particularly of those other persons who were not connected with the case, could well be affected.
>
> Nonetheless, I was convinced that there was a genuine need to obtain such important evidence in enforcing the law. Carefully and thoroughly considering the matter, I considered that it was proper and lawful means to obtain evidence of corruption and gave verbal approval to coverty tape record the meeting at Langham Hotel on the evening of 4 November 2003 and asked Mr. Patrick Ho to make the necessary arrangements to follow up.[77]

Without any outside observer to confirm this account and, in this case, no written record of Mr. Lui's decision-making process, it is impossible to know to what extent Mr. Lui considered the Article 14 rights of the individuals being investigated, and whether it was in fact as deliberate and as "thorough" as Mr. Lui later claimed. In the absence of any outside oversight, reviewing or even understanding the process of balancing the individual's right to privacy with the state's responsibility to protect public security and investigate crimes becomes impossible. In such situations, both Article 14 of the BORO and Article 30 of the Basic Law protect individual privacy only as much as the investigating officer decides that they do.

Judge Sweeney was clearly troubled by the lack of any external oversight:

> Clearly, the whole process is carried out without reference to any outside body and allows of [sic] no right of inspection or appeal. Indeed, it can fairly be said that the only protection the citizen has against such unfettered and supervised power is the goodwill of the principal investigator.[78]

The question, then, according to the judge, is whether or not such a bare-bones process, existing at the lower end of Hong Kong's legal hierarchy, could be said to be "in accordance with legal procedures," in compliance with Article 30 of the Basic Law.

[77] Ibid., paragraph 20.
[78] Ibid., paragraph 22.

In his analysis, Judge Sweeney relied heavily on European Court of Human Rights decision in *Malone v. United Kingdom*.[79] In *Malone*, the ECHR pointed out that he *quality* of the law, not just its mere existence, must be addressed.[80] In particular, the ECHR pointed out that "there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by [the right to privacy]."[81]

The ECHR did not create a list of procedural requirements that a law should have in order to pass muster under Article 8. Instead, it merely emphasized that the law must give sufficiently specific direction so as to ensure that the grant of discretion to the police officer is not "arbitrary." Similarly, Judge Sweeney did not lay down a list of specific requirements. Instead, he pointed to the creation of the Regulation of Investigatory Powers Act (RIPA) in the UK, which "provide(s) detailed rules for the authorization of covert surveillance as well as its documentation in writing and retention of such material for subsequent inspection."[82]

Judge Sweeney did mention one specific procedural requirement that of central importance: judicially-issued warrants, similar to those issued for physical searches.

> Just as the relevant authorities must apply for a search warrant before they can invade the privacy of one's home, I can see no valid reason why they should not also be obliged to apply for some form of warrant before they can invade the privacy of personal communications.[83]

Because no such framework exists in Hong Kong that is sufficiently protective of the right to privacy under Article 30, the judge held that there is a "legislative lacuna."[84]

Judge Sweeney's reference to the UK RIPA law, and his specific discussion of judicial warrants, give some indication of what is required for a law to pass muster under Article 30 of the Basic Law. If, for example, the government were to merely create legislation that in every respect mirrored the pre-existing system, it is unlikely that such a law would be of sufficient "quality." Given the lack of procedural safeguards in the August 2005 Executive Order, it is unclear whether the current framework itself satisfies the requirements of Article 30.

Despite the violation of the defendants' Article 30 rights by the ICAC investigators, the judge held that the recordings were in fact admissible as evidence. Following British Commonwealth and European Court of Human Rights precedent that permits the

---

[79] *Malone v. the United Kingdom*, [1984] ECHR 10, 2 August 1984. Although the *Malone* case concerned phone taps, its logic has been applied to covert surveillance. See *Khan v. United Kingdom*, [2000] ECHR 194, 12 May 2000.
[80] *Malone v. the United Kingdom*, [1984] ECHR 10, 2 August 1984, paragraph 66.
[81] *Malone v. the United Kingdom*, [1984] ECHR 10, 2 August 1984, paragraph 67.
[82] *HKSAR v. Li Man Tak and Others*, Criminal Case No. 689 of 2004, 22 April 2005, [2005] HKEC 1308, paragraph 53.
[83] Ibid., paragraph 56.
[84] Ibid., paragraph 54.

introduction of unlawfully obtained evidence unless doing so would make a fair trial impossible, the court allowed the prosecution to use the evidence. In doing so, it rejected an American-style exclusionary rule for evidence that is unlawfully obtained.

Crucially, the court also held that any future covert surveillance might well be in bad faith. Because the government is now aware of the "lacuna", or gap, in the law, it could no longer delay legislative action:

> 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, and unless and until this ruling is overturned, 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.[85]

In other words, the hole in the law would have to be addressed before the practice of covert surveillance could be continued.

The Shum Chiu case

Also forcing the government's hand was the decision in the July 2005 *Shum Chiu* case.[86] In the *Shum Chiu* case, unlike the *Li* case, the judge, District Court Deputy Judge Julia Livesey actually threw out the evidence against the accused, a group of Hong Kong businessmen accused of conspiracy to bribe a government official. In fact, she ordered an end to the proceedings, on the grounds that a fair trial could no longer be guaranteed.

But the decision to end proceedings against the men had little to do with the gap in the law. Instead, the court focused on the substance of the conversations being surreptitiously observed and recorded. In an attempt to acquire more evidence against some of the conspirators, the ICAC arranged to record a meeting between the conspirators and their lawyer, meeting after the first arrests by the ICAC in the case. The ICAC arranged to record the meeting despite knowing, in advance, that legal counsel would be present, and that they were meeting specifically to discuss the ICAC investigation.[87]

The judge was clear in her determination of the situation:

> From the facts above, the only inference which, in my judgment, can be drawn is that the ICAC deliberately and intentionally recorded a conversation between [one of the defendants] and his solicitors, knowing that legal advice would almost certainly be given and would almost certainly cover matters relating to the raid, which meeting would, therefore, be *prima facie* privileged.[88]

[85] Ibid., paragraph 67.
[86] *HKSAR v. Shum Chiu and Others*, Criminal Case no. DCCC 687 of 2004, 5 July 2005.
[87] Ibid., paragraph 8(f).
[88] Ibid., paragraph 13.

Under such circumstances, the judge held, the case against the defendants would have to be discontinued. The fact that the ICAC had listened in on the conversation seriously prejudiced the defendants' right to a fair trial, and there was no way to remedy the violation save for ending the prosecution.

Although the outcome in the case would have likely been the same even without the issue of the lack of a proper legislative framework for covert surveillance, Judge Livesey did mention the problem at the end of her opinion:

> The legislators also need to introduce the regulations required for lawful covert recording, *as was originally envisaged under the Basic Law*. They should do so with all due haste, so that the guarding of the guards is not just left to the Judiciary.[89]

The *Shum Chiu* case demonstrates how a proper legal regime, which the appropriate checks and balances, can save an investigation from a fatal mistake. Had the ICAC been forced to seek outside prior approval, then the outside authority would have almost certainly saved the investigation from itself by denying the inappropriate request.

VI. The Executive Order

Within a month of the decision in the *Shum Chiu* case, the government issued an Executive Order empowering all government departments which "undertake law enforcement investigations or operations" to engage in covert surveillance.[90] The Order, which was announced on August 5, 2005, was very weak in terms of its procedural safeguards, and did little to allay the fears of those who were concerned about the government's plans for handling the issue.

As noted above, under the Executive Order, surveillance can only be carried out after authorization from a sufficiently senior officer of the department, one specifically designated by the department head to review such requests.[91] Although each department head must also name a second officer to review, from time to time, authorizations under the Executive Order, that review is after the fact, and no mechanism was created to allow for outside review. No other procedural safeguards were put in place.

Authorization could be granted as long as the surveillance was for the purpose of "preventing or detecting crime" – there was no limitation that the crime be "serious" – and "protecting public safety and security," which was not further defined.[92] This provision raised concerns that the government was seeking to create legal authority for the government to engage in political surveillance under the guise of protecting state security.

---

[89] Ibid., paragraph 53. Emphasis added.
[90] Law Enforcement (Covert Surveillance Procedures) Order, Section 2(1), July 30, 2005.
[91] Law Enforcement (Covert Surveillance Procedures) Order, Part 5, Section 15, July 30, 2005.
[92] Law Enforcement (Covert Surveillance Procedures) Order, Sections 3(a)(i) and (ii).

Rather than a straight requirement that the surveillance produce information of "substantial value," instead the Executive Order calls for a potentially more permissive balancing test, in which "the need for covert surveillance" is balanced 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."[93] Finally the Executive Order creates a balancing test for the use of less intrusive means, rather than creating a clear requirement that less intrusive means not be available.[94]

The government claimed the power to issue the order under Article 48(4) of the Basic Law, which authorizes the Chief Executive to "decide on government policies and to issue executive orders." It claimed that the text of Article 30 allows for government surveillance of communication "in accordance with *legal procedures* to meet the needs… of investigation into criminal offences."

Under the government's reading, the use of the phrase "legal procedures" permits the use of executive orders in this context. In the government's words:

> (The government) accepts that the constraints it places on law enforcement officers are not "prescribed by law."
>
> However, a court has previously decided that "when the Basic Law contemplates that a particular course of action has to be prescribed by law, the Basic Law says so." The fact that Article 30 speaks of "legal procedures" therefore indicates that a meaning other than prescribed by law" was intended.[95]

This reading cuts against the first sentence in Article 30, which states that "(t)he freedom and privacy of communication of Hong Kong residents shall be protected by *law*." Also working against the government is Article 39 of the Basic Law, which states that "(t)he rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law."[96] The first sentence of Article 30 is the key sentence: it calls for laws to protect the right to privacy, and the second sentence allows the government to engage in surveillance for certain reasons *as empowered by law*. In relying on the "legal provisions" language of Article 30, the government has put the cart before the horse.

The government can, and should, implement "legal procedures" that describe in detail the process for engaging in covert surveillance, but these legal procedures should be based on legislation enacted by LegCo that empowers the government to do so. As the Hong Kong Bar Association put it:

---

[93] Law Enforcement (Covert Surveillance Procedures) Order, Section 3(b)(i).
[94] Law Enforcement (Covert Surveillance Procedures) Order, Section 3(b)(ii).
[95] Ian Wingfield, "Covert surveillance order necessary," Hong Kong Government Statement, August 11, 2005.
[96] Hong Kong Basic Law, Article 39(2).

> The order purports to make lawful what may otherwise be unlawful by requiring prior authorization to carry out covert surveillance. That is quintessential lawmaking. That is what a law made to implement Article 30 [of the] Basic Law can do but an executive order cannot.[97]

The government's approach of dealing with the issue through an executive order undermines the separation of powers created by Hong Kong's Basic Law. Hong Kong has a *de facto* executive-led government. Governmental power is heavily concentrated in the hands of the Chief Executive: the government bureaucracy is largely under executive control, and is not politically accountable to LegCo.[98] The Chief Executive can independently introduce legislation without, as in some other executive-led political systems, finding an elected legislator as his surrogate. At present, until the courts of Hong Kong have a chance to weigh in on this practice, she or he is not obligated to act on legislation enacted by the legislature, to either sign it or send it back with a veto.[99]

For this reason more than any other, the protections in Hong Kong's Basic Law against governmental intrusions on individual rights, and its key limitations on executive power, are absolutely crucial to the preservation of human rights and the rule of law in Hong Kong. Although the Chief Executive's powers outweigh those of the Legislative Council and the judiciary, his authority is still checked in key ways by the Basic Law.

The Executive Order undercut the balance of powers laid out in the Basic Law, and should therefore be withdrawn by the government as an unconstitutional encroachment on the Legislative Council's legislative authority.

Not only is the Hong Kong government obliged under Article 30 of the Basic Law to introduce legislation on covert surveillance – rather than dealing with it through an executive order – it is also obliged to do so according to its obligations under international law.

Article 39 of the Basic Law makes clear that the protections of the International Covenant on Civil and Political Rights apply to Hong Kong. Article 17 of the ICCPR protects the right to privacy from governmental interference. The United Nations Human Rights Committee, which has primary authority over the interpretation of the ICCPR, made clear in its general commentary on Article 17 that the right to privacy can only be infringed in accordance with sufficiently protective state *law*.[100]

---

[97] Hong Kong Bar Association, *Law Enforcement (Covert Surveillance Procedures) Order: Statement of the Hong Kong Bar Association*, 8 August 2005, paragraph 7.

[98] Although Article 64 of the basic law refers to the government's "accountability" to LegCo, Article 99 of the Basic Law makes clear that the bureaucracy is "responsible to the Government of the Hong Kong Special Administrative Region."

[99] Although the Article 43 of the Basic Law includes among the Chief Executive's functions the responsibility to "sign bills passed by the Legislative Council and to promulgate laws," the scope – and limiting power – of this provision has yet to be judicially determined. It may be so in litigation currently before Hong Kong's courts.

[100] The commentary states that, "(t)he primary method of providing such protection is state legislation. No interference may take place except in cases envisaged by the law."

The Human Rights Committee expanded on its initial commentary in a second comment in 1988, again making clear that intrusions on the right to privacy had to be both specified by law and also precise and narrowly-tailored:

> Even with regard to interferences that conform to the Covenant, *relevant legislation* must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis. … States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.[101]

In order to remedy the its non-compliance, the government should withdraw the Executive Order immediately and seek to remedy the gap in the law through legislation, drawn up in coordination with the LegCo.

A question of timing?

According to the government, issuing an executive order that allowed for judicial approval of covert surveillance warrants was impossible. In the government's view, all that was possible was maintenance of the status quo:

> In any event, it would not have been possible to include a judicial monitoring system in the Executive Order, since the Chief Executive cannot by such an order give powers to, or impose functions on, members of the independent Judiciary.[102]

But the government's move to issue an executive order was belied by the fact other options were – and still are – available. More than three months passed between the decision in the *Shum Chiu* case and the making of the Executive Order, more than enough time for the executive to work with the Legislative Council to come up with a stop-gap solution to the problem, such as temporary legislation that could authorize covert surveillance until more formal legislation could be passed.

Given the intense amount of study that has been devoted to the issue – by the Law Commission, by the Hong Kong Bar Association, by the government, and by LegCo, all of whom have been dealing with and waiting on this issue for years – LegCo could have responded quickly to any government bill. As far back as April 1997, the Hong Kong Bar Association pointed out that, given the already-significant amount of internal and public discussion, the government could move directly to legislation, especially given that the

[101] General Comment 16/3/2 of 23 March 1988, paragraphs 8 and 9; Hong Kong Law Reform Commission, Privacy Law, paragraph 22. Emphasis added.
[102] Ian Wingfield, "Covert Surveillance order necessary," Hong Kong Government Statement, August 11, 2005.

need for legislation was "urgent."[103] Instead of taking advantage of this vast expertise and experience, the government dealt with the matter internally, with no public consultation, and no consultation with the public's representatives in LegCo.

Chief Executive Tsang has claimed that the executive order is not a grant of additional power. Rather, he claimed, it is merely a "clarification" of the ability of law enforcement agents to eavesdrop on Hong Kong residents:

> What I wish to emphasize is that first this order does not add anything to the power currently exercised by our law enforcement bodies. It simply clarifies what they are allowed to do. In fact it limits their power in the sense that only very senior officers will be able to invoke this particular power.[104]

In a sense, this is true: Hong Kong's law enforcement agencies engaged in covert surveillance before the April and July 2005 court decisions, and they are now empowered to continue to do so. What has changed is that the Chief Executive has given his imprimatur to a covert surveillance scheme that does not have the minimum safeguards necessary to ensure against abuse.

Though the government has called the executive order a mere "temporary measure," it has shown no hurry to introduce legislation to take its place. During a meeting with a group of Hong Kong legislators in August 2005, Secretary for Security Ambrose Lee announced that there would be no movement toward a new law for at least six months.[105] At that late-August meeting, Secretary Lee told the LegCo members that legislation would not be introduced until February or March 2006.

The government's issuance of the Executive Order, and its claim that it needs six months to study the problem, belies the fact that the issue has been waiting for government action for years. At least since the passage of the BORO fifteen years ago, the Hong Kong government, both pre- and post-handover, has known that about the lack of sufficient legislation in this area. The court cases, rather than taking the government by surprise, merely took the option of continued delay off the table.

Why the delay?

Given that the post-handover government had more than eight years to deal with this issue, why has it consistently failed to do so? Certain factors seem to have played at least some role in the government's decision-making process.

One likely factor was the unwillingness of an incoming government, under extremely close scrutiny for any signs of backsliding on human rights, to introduce legislation on

---

[103] Hong Kong Bar Association, *Submission of the Hong Kong Bar Association on the Consultation Paper on Interception of Communications Bill*, 2 April 1997, paragraphs 1-2.
[104] Hong Kong government transcript of remarks by Chief Executive, August 6, 2005.
[105] Dennis Chong, "Long wait for wiretap law," Hong Kong *Standard*, August 24, 2005.

such a sensitive issue. Government power to engage in covert surveillance cuts to the heart of the question of the proper balance between individual rights and the need for the government to have the requisite powers to carry out its police function. Many governments, when faced with a politically-sensitive issue, choose inaction over politically risky and potentially costly action.

The government might be especially unwilling to have that conversation if it believes that its position on covert surveillance strikes a balance that favors the government. "If you are a police officer or working for ICAC, then the system is working pretty well," one lawyer commented.[106]

As Legislative Councillor James To put it:

> The power is in their hands. It was possible that, with review, with legislation, they would lose full power, and could end up with court involvement. You may as well not trigger that process yourself.[107]

Another factor, unforeseen by the government, contributed to the continued delay: the implosion of the government's Article 23 national security legislation, culminating with its ultimate withdrawal for further "consultation" in September 2003.[108] The government's initial Article 23 proposals, introduced on September 24, 2002, were flawed in a number of areas, and in several instances, sacrificed individual rights protections in favor of greater government latitude to investigate and prosecute.[109] The poor quality and overall retrograde nature of the proposals, as well as the government's politically tone-deaf approach to selling its wares to the public, led to the eventual demise of the proposed legislation, and, eventually, to the early resignation of the first SAR Chief Executive, Tung Chee-hwa.

In the immediate aftermath of the Article 23 debacle, the government had to be wary of any further legislation that could be perceived as a threat to civil liberties. "If you had your nose bloodied on Article 23 like they did, then you might be hesitant to bring something like this forward," said one Hong Kong lawyer who followed the Article 23 debate very closely.[110]

VII. Conclusion: leaving the courts out?

Less than two weeks after the issuance of the Executive Order, Hong Kong got its first glimpse of what the government's proposed legislation might look like. On August 16, the Hong Kong *Standard* carried an article which claimed to describe the government's plans for a covert surveillance bill. Contrary to some predictions, the government will

[106] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.
[107] Hong Kong Human Rights Monitor interview with James To, Hong Kong, October 2005.
[108] "Hong Kong withdraws National Security Bill," *China Daily*, September 5, 2003.
[109] For more on the government's Article 23 proposals, see Thomas E. Kellogg, "Legislating Rights: Basic Law Article 23, National Security, and Human Rights in Hong Kong," *Columbia Journal of Asian Law*, May 2004.
[110] Hong Kong Human Rights Monitor interview, Hong Kong, October 2005.

introduce legislation that allows for judicial review of covert surveillance requests in all criminal cases, the *Standard* reported. If true, this would represent a major step forward.

However, the *Standard* also reported that the government will seek the power to authorize wiretaps on its own in cases regarding state security. "We cannot seek court approval in every case and expose the case's details just for the sake of good governance," one senior official said.[111]

But rules requiring court approval are not put in place merely for the sake of an abstract notion of "good governance." Rather, they exist in order to ensure against the abuse of power by those who hold it. The comments of the unnamed senior official suggest that the Hong Kong government may seek to create a two-track system for regulation of electronic surveillance: one track would cover the use of electronic surveillance by law enforcement officials, and also, presumably, the ICAC, and would require that these agencies seek a judicially-authorized warrant before engaging in any such surveillance. The second track would be reserved for any surveillance carried out for the purposes of "national security," against either domestic or foreign agents.

To push for such a system would be a major mistake. Outside oversight is the best insurance against abuse of power, and there is no reason why courts cannot exercise that function, even on matters of state security. As the Supreme Court of the United States pointed out:

> We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. ... There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. ... If the threat is too subtle or complex for our senior enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.[112]

As noted above, little is known about Hong Kong's state security apparatus, and there is little publicly-available information about the Hong Kong government's use of electronic surveillance for state security purposes. The government needs to place that apparatus

---

[111] Carrie Chan, "Surveillance debate may explode in Tsang's face," Hong Kong *Standard*, August 16, 2005.

[112] *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), 320. In *Keith*, the Supreme Court ruled that there was no "national security exception" to the warrant requirement in terms of government surveillance of domestic groups engaged in activities that are allegedly an affront to national security. Even under such circumstances, the court said, law enforcement agencies needed to seek out a warrant before engaging in any surveillance of individuals or groups that it believed were engaging in activities that were a threat to national security. In the wake of the September 11, 2001, terrorist attacks on the United States, certain changes to the legislative framework governing the conduct and oversight of electronic surveillance by US government agencies were enacted, although the baseline requirement of judicial authorization in most cases remained in place. A detailed discussion of the US framework and the post-9/11 alterations to it is beyond the scope of this document; for a detailed discussion of both issues, see Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*, CRS Report for Congress, Library of Congress, September 22, 2004.

under an appropriate legal regime, and take steps to ensure proper legislative and judicial oversight. Both steps can be taken without jeopardizing the security and stability of Hong Kong.

The government's years of inaction, and its decision to temporarily foreclose, by executive order, any legislative input, betrays an unfounded lack of trust in the other branches of government in Hong Kong. The government should have enough confidence in the Legislative Council to work with it to create the best legislation possible, just as it should trust Hong Kong's judiciary to act fairly and objectively when presented with a request to engage in surveillance under any new law.

If the government does that, then the people of Hong Kong will more fully trust it to use the power granted to it under any new covert surveillance law sparingly, in accordance with the Basic Law. The preservation of that public trust should be the government's ultimate goal.