

A Flawed Effort? Legislating on Surveillance in Hong Kong

By Thomas E. Kellogg

Hong Kong Journal, Issue no. 6, April 2007

On August 6, 2006, at the end of a record-setting 57 ½ hour legislative session, the Hong Kong Legislative Council, or Legco, passed a historic bill regulating the use of the interception of communications and covert surveillance by Hong Kong authorities. The new law on electronic surveillance – which includes both wiretapping and bugging, among other techniques – is an important step forward in that, for the first time in Hong Kong's history, these are covered by law. Many forms of electronic surveillance will require authorization from a member of a three-judge panel created specifically to review such requests.¹

Yet while the law itself is an important milestone, it is far from perfect: it lacks clear limiting definitions for key terms, and its oversight mechanisms were criticized by some in Legco as being too weak. Just as important, some government actions in drafting the bill and getting it passed showed an unwillingness to engage fully with Legco's pan-democratic parties, despite the fact that they represent a clear majority of the voting public. In the final Legco debate, pro-government legislators either voted down or had ruled out of order nearly 200 proposed amendments put forward to strengthen the bill's human rights protections.

In some ways, the government's handling of electronic surveillance legislation may be instructive. It may signal the ways by which the government seeks to handle human rights-related issues in the future, including much-anticipated new proposals on national security under Article 23 of the Basic Law (Hong Kong's *de facto* constitution). An overview of the process by which the Interception of Communications and Surveillance Ordinance came into being therefore suggests how the pan-democratic parties might influence future government policy on key human rights legislation more effectively.

Before the Surveillance Ordinance was passed, Hong Kong was one of a small number of first world jurisdictions that did not regulate electronic surveillance by the government. For decades, its British colonial government refused to legislate and, during its first eight years in power, the SAR government followed suit, ignoring calls for action from legislators and activists.

The basic concept is this: because electronic surveillance is so intrusive, the state must create basic safeguards to ensure that all citizens' privacy rights are protected. In general, most jurisdictions have viewed judicial oversight, usually in the form of a warrant, as the best way to protect individual privacy rights while ensuring that the state can use surveillance technology when necessary to investigate alleged criminal activity. This basic concept was given short shrift by successive administrations despite the fact that both the Hong Kong Bill of Rights Ordinance, passed in 1991, and the Basic Law, protect the right to privacy. Hong Kong's responsibilities under the International Covenant on Civil and Political Rights (ICCPR) also should have spurred the government to action.

Electronic surveillance not only puts individual privacy at risk, it is also prone to potential abuse. Governments around the world too often have been tempted to use the tools of electronic surveillance to spy on political enemies or other non-violent political activists. Although the full extent of such surveillance has never been fully disclosed, the Hong Kong government, both before and after 1997, has been plagued by accusations of misuse and abuse of its electronic surveillance power. In the 1980s, the British colonial government was embarrassed by media reports that local political activists, including longtime public figures Frank Ching, Anna Wu and Christine Loh, had their phones tapped by a special secret government committee. After the handover, many pro-democratic activists and legislators voiced suspicions that their conversations have been monitored but, as yet, no concrete evidence has emerged to validate these claims.

Judicial oversight: forcing the government's hand

The problem was brought to the fore by a district court judge's decision in April 2005. In that case, *HKSAR v. Li Man Tak and Others*, the government was prosecuting a group of Hong Kong businessmen for corruption. Hong Kong's Independent Commission Against Corruption (ICAC), which from its inception in the mid-1970s has wielded extensive investigatory powers, had in the course of its investigation bugged two restaurants where the businessmen met, allegedly to discuss various issues related to their illegal activities. While the judge in the case, the soon-to-retire Judge Fergal Sweeney, allowed the ICAC evidence to be used, he indicated that, without a proper legislative basis, evidence collected in future cases by use of electronic surveillance could be disallowed.

In a case decided less than four months later, *HKSAR v. Shum Chiu and Others*, a district court actually threw out evidence collected by the ICAC through use of covert surveillance. In that case, it had recorded a meeting between the individuals being investigated and their lawyer, thereby severely infringing their right to seek confidential legal counsel. The court both reprimanded the ICAC for recording what should have been a privileged conversation, and repeated the call made in the Li Man Tak case for new legislation on the government's use of electronic surveillance.

The government initially responded not with a draft bill, as had been expected, but with a so-called executive order which purported to provide a temporary legal basis for the use of electronic surveillance while work continued on permanent legislation. The executive order was generally weak on procedural or other safeguards, and did not allow for any judicial role in the authorization of wiretaps or bugs. Soon after the order was issued, it was challenged in court by political activists Leung Kwok Hung, also known as "Long Hair," and Koo Sze Yiu, on the grounds that it was in fact an act of lawmaking—something the government, even in executive-led Hong Kong, was not empowered to do. On February 9, 2006, Justice Michael Hartmann of the High Court ruled against the government, declaring the Executive Order unconstitutional and setting a six-month deadline for the enactment of legislation, after which all electronic surveillance would be deemed without sufficient legal basis.

There is much to praise about the government's response to these losses: it chose to abide by both rulings rather than appeal to Beijing for aid, as it did in the infamous 1999 "right of abode" case and the 2005 interpretation on the Chief Executive's term of office under the Basic Law. In doing so, the government avoided creating a high-profile and highly controversial dispute over Beijing's authority to intervene.

The government also avoided many of the mistakes it had made during its failed 2004 push to pass Article 23 legislation, widely viewed as playing a key role in bringing an early end to the administration of Chief Executive Tung Chee-hwa. During the Article 23 debate, government spokespeople often took a combative stance toward its critics, and failed to allay public fears over the bill's shortcomings. At one point, then-Secretary for Security Regina Ip seemed to denigrate the public's ability to comprehend the government's proposals, saying that "taxi drivers, restaurant waiters, and workers at McDonald's" did not need to see the text of the government's proposals, and that such calls were coming only from a handful of "experts."²

The government did not repeat these mistakes while drafting and selling its electronic surveillance proposals. In general, it struck a moderate tone and tried to avoid making headlines. Though it refused to allow a public consultation period for public feedback, the government did hold discussions with at least one local NGO during the legal drafting phase.³

Yet for all of its improved public relations, the government refused to engage in any serious way with the pan-democratic parties over possible changes to the bill once it released a draft in early March 2006. The draft made clear that concerns of pro-democratic legislators, many of whom responded in detail to the government's first proposals in late February, had not been addressed. "We want to cooperate but, even knowing our concerns, they haven't taken them into account in this bill," said prominent lawmaker Audrey Eu after seeing the draft bill. "Obviously that makes the [legislative] process much more difficult."⁴

Instead, the government took advantage of public complacency and remained confident that its pro-government majority in Legco would deliver a final product largely similar to its own first draft. In doing

so, it ignored not only the reform proposals of pro-democratic legislators but also many suggestions from the Hong Kong Bar Association, which called the government's draft inconsistent with "the guarantees (of) fundamental rights and freedoms under... the Basic Law and the ICCPR." It also suggested that "more time (be) devoted to exploring legislative options" different from the government's proposals. This call for broader discussion was also brushed aside.⁵

While public opinion failed to coalesce in ways that forced the government to reconsider its approach, nonetheless there were indicators that its proposals were meeting with some dissatisfaction. According to a survey of 300 Hong Kong residents carried out in early July 2006 by the *South China Morning Post*, a strong majority of residents had significant concerns about the government's bill. A full 72% of those polled said they would prefer having judges who would oversee wiretapping requests be picked by the Chief Justice rather than by the Chief Executive, as in the government draft. A majority also supported expanding the law to cover electronic surveillance by mainland agencies.⁶

From bill to law: a missed opportunity?

In part as a result of this refusal to listen to critics, the final bill contains several weaknesses that remained unaddressed. In a number of ways, the ordinance, while incorporating the key safeguards of judicial oversight and a specially-created commissioner to oversee the approval and use of electronic surveillance, falls short of legislation on the books in other Commonwealth jurisdictions and in the United States. In general, as the Bar Association and others pointed out, the government based its draft legislation largely on British and Australian law, even though neither country has a long history of protecting basic rights through constitutional mechanisms. Given Hong Kong's commitments under the ICCPR and its own Basic Law, it is unclear whether these models were the best choice.

Under the Surveillance Ordinance, all wiretapping and some other forms of electronic surveillance, particularly those that require law enforcement officials to enter an individual's home or office secretly to install listening devices, must be approved by one member of a specially-appointed three-judge panel. Other forms of electronic surveillance are approved administratively, by a high-ranking officer within the department engaged in surveillance. Electronic surveillance can only be approved for the investigation of "serious crimes" and for alleged threats to "public security."

For such requests to be approved, the officials seeking authorization must articulate a "reasonable suspicion" that the individual in question has been or will be engaged in criminal activity. In addition, judges and government officials are supposed to balance the intrusiveness of the proposed surveillance against the seriousness of the crime being investigated and the value of any information likely to be obtained.

The main safeguard against abuse of this surveillance power is the creation of a Commissioner on Interception of Communications and Surveillance. Under the law, the Commissioner is empowered to investigate allegations of misuse of this authority by government officials, and is empowered to investigate claims by members of the public that they have been inappropriately monitored. The Commissioner must publish an annual report on the use of electronic surveillance by government bureaus, giving both the Chief Executive and the public some sense of the scope of its use. Importantly, however, the Commissioner cannot overrule a decision to engage in electronic surveillance; he can only inform the Chief Executive that he or she believes that a problem exists.

The most troubling aspect of the new law is that it covers only Hong Kong government entities; both foreign and mainland Chinese entities are left untouched by it. In general, the regulation of electronic surveillance by other governments is not an issue in most legal jurisdictions: any such activities generally would be considered espionage and would be subject to serious criminal sanctions. But, given Hong Kong's special status as a Special Administrative Region of the PRC, there is a need to define Beijing's powers and responsibilities under the law. This is especially so given that many observers believe that Beijing increased its own political monitoring of Hong Kong in the wake of the July 1, 2003 protests, which brought some 500,000 Hong Kong citizens to the streets and caught both the SAR government and

Zhongnanhai off guard. 7 While activities of the PRC state security forces in Hong Kong are a sensitive issue, nonetheless they need to be addressed. That would let all Hong Kong citizens know they are fully protected from unlawful intrusions into their privacy from any and all sources.

Another problematic aspect of the surveillance law is that it empowers the government to engage in electronic surveillance to protect “public security.” Because such terms are so elastic, many governments have defined them carefully to prevent abuse. Though the Hong Kong government did include a clause stating that its surveillance power should not be used to monitor dissent, it declined to narrow further its reference to public security. Given the extensive number of comparative legal examples on which to draw, it is difficult to understand why the government did not address this key issue.

Finally, the law creates a system in which panel members, though referred to as “judges,” lack sufficient distance from the executive branch. They are appointed by the Chief Executive, rather than the Chief Justice, and the law makes explicitly clear that they are not to be considered judges for the purposes of the Surveillance Ordinance. As legislator Margaret Ng has pointed out, the Surveillance Ordinance system differs from the approach taken by the US, the UK, and Australia, all of which seek to preserve the key principle of separation of powers in their laws on wiretapping and other forms of surveillance.⁸

All of these weaknesses may lead to situations in which the police, not sufficiently pushed by the law's approval mechanisms, turn to electronic surveillance in early stages of their investigations. As a result, the government may end up tapping the phones of innocent citizens – politically-connected or not – whose only crime is to have come under government suspicion by mistake. In many ways, rigorous supervision of police powers gives the police an incentive to do their job well, making it less likely that tapping a private citizen's phone will happen in error.

In sum, the final text of the Surveillance Ordinance reveals a government that, while willing to adhere to the minimum requirements of international and comparative law, nonetheless is not interested in a more active approach to the protection of individual rights. The enactment process showed that the government feels no special obligation to engage with the political opposition, and is willing to take full advantage of an election system that falls far short of one person, one vote.

The passage of the Surveillance Ordinance into law raises serious concerns that the Tsang government will carry this approach into future battles over legislation that directly impacts human rights. If the government continues to prioritize public relations over legislative quality, then the pro-democratic parties will be faced with a serious dilemma: how does one advance reforms when the government refuses to negotiate, secure in its knowledge that the electoral system shields it from the full brunt of legislative decisions?

For the pro-democratic parties, the lessons are twofold: first, it is now dealing with a government that, on key issues at least, is less likely to allow self-inflicted wounds to derail its legislative agenda. Second, public opinion is key: unless the pan-democrats can demonstrate that both the government and its Legco supporters will pay a price in the court of public opinion for refusing to negotiate, then they may find that the government is more than happy to follow its own prerogatives. In other words, quality proposals in themselves may not be enough to nudge the government to the bargaining table.

As finally enacted, the Surveillance Ordinance is no tragedy. It is, however, a disappointment. The government can justifiably take pride in the fact that, for the first time in Hong Kong's history, the use of electronic surveillance is covered by law. But the government's failure to listen to those in the democratic camp regarding amendments that could have strengthened that law means that the legislation as finally passed is not as strong as it could have been. In the final analysis, political victories for the government in the legislative process may in fact leave the people of Hong Kong, who must rely on this law to protect their rights, that much poorer.

Thomas E. Kellogg is a senior fellow at Yale University's China Law Center and a lecturer at the Yale Law School. A graduate of Harvard Law School, he has worked for a wide range of non-governmental organizations in the United States, Asia and the Middle East, focusing on human rights and the development of the rule of law.

1. In general, "interception of communications" refers to the tapping of telephones and other methods of intercepting communications between two private individuals. "Covert surveillance" refers to the use of technology in order to listen in on a conversation between two or more persons. One of the most common forms of covert surveillance is bugging, but the term covers a range of other techniques. For the purposes of this Article, the author uses the term "electronic surveillance" to encompass both interception of communications and covert surveillance.

2. Tom Kellogg, "Legislating Rights: Basic Law Article 23, National Security, and Human Rights in Hong Kong," 17 *Columbia Journal of Asian Law* 307, 358 (2004).

3. Disclosure: the author took part in this meeting as a legal advisor to that NGO, the Hong Kong Human Rights Monitor. The Hong Kong Human Rights Monitor's recommendations to the government on the regulation of electronic surveillance, published as a briefing paper in October 2005, were also largely rejected by the government. See HKHRM, *Surveillance, Basic Law Article 30, and the Right to Privacy in Hong Kong*, available online at: <http://www.legco.gov.hk/yr05-06/english/panels/se/papers/secb2-259-1e.pdf>.

4. Ravina Shamdasani and Benjamin Wong, "Warning as critics of snooping bill are snubbed; lack of concessions makes it hard for spy rules to pass Legco, say democrats," *South China Morning Post*, March 2, 2006.

5. See "Interception of Communications and Surveillance Bill: Comments of the Hong Kong Bar Association," March 24, 2006; available online at: <http://www.hkba.org/whatsnew/submission-position-papers/2006/20060324.pdf>.

6. "Survey says snooping law should offer more protection," *South China Morning Post*, Monday, July 3, 2006.

7. Keith Bradsher, "Hong Kong Legislators Pass Sweeping Surveillance Bill," *New York Times*, August 7, 2006.

8. Margaret Ng, "Will the judiciary stand up to the new test?," *South China Morning Post*, September 5, 2006.