

LC Paper No. CB(2) 2607/05-06(01)

Prescott Beighley

**Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong**

Tel: 852 2358 7689 (voice) 852 2358 1749 (fax) e-mail: scottb@ust.hk

26th June 2006

Hon James TO Kun-sun
Room 409, West Wing
Central Government Offices
Hong Kong

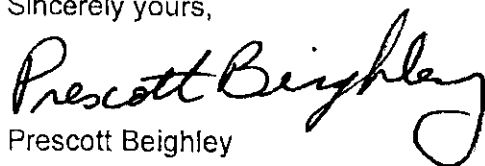
Dear Mr TO,

In view of your role as a member of the Legco Bills Committee on the Interception of Communications and Surveillance Bill and as Chairman of the Panel on Security, I am enclosing a brief paper that I believe is relevant to the covert surveillance matters currently before Legco.

As noted in the paper, not only do current surveillance technologies involve a level of sophistication that is heretofore unprecedented, they also involve levels of privacy invasion and health concerns the likes of which have never been seen before. And while technical surveillance may be covert and passively applied to monitoring the activities of target individuals, surveillance technologies can also be used for electronic harassment and mind control purposes.

It is my sincere belief that the members of Legco should be aware of these matters and take them into consideration in formulating relevant legislation.

Sincerely yours,



Prescott Beighley

Adjunct Professor, Hong Kong University of Science and Technology
Hong Kong resident since September 2003
U.S. citizen and passport holder

Technical Covert Surveillance in Hong Kong

Draft, 26 June 2006

I. Background

The matter of covert surveillance is currently before Legco in connection with the enactment of legislation governing the powers that Hong Kong security agencies shall have in conducting such surveillance activities. The purpose of this paper is to highlight recent developments and practices in technical covert surveillance that legislators and policy makers may want to take into consideration in formulating laws and policies.

II. Review of technical surveillance technology and its applications

Surveillance may be described as follows:

Surveillance is the art of watching over the activities of persons or groups from a position of higher authority. Surveillance may be covert (without their knowledge) or overt (perhaps with frequent reminders such as "we are watching over you"). Surveillance has been an intrinsic part of human history. Sun Tzu's *The Art of War*, written 2,500 years ago, discusses how spies should be used against a person's enemies. But modern electronic and computer technology have given surveillance a whole new field of operation. Surveillance can be automated using computers, and people leave extensive records that describe their activities.¹

A. Technical surveillance technology and capabilities

Surveillance involving electronic and computer technology can be thought of as technical surveillance. While information about the technology used in covert technical surveillance is unclassified and generally available to the public, much of it is reportedly classified and known only to select government agencies.

1. U.S. Congress Office of Technical Assessment Report (1988)

In May 1988 the Office of Technological Assessment of the U.S. Congress published a special report entitled "New Technologies and the Constitution." The main subject of the report is technology and rights in criminal justice.

The report states that

In the last two decades, advances in imaging technology, remote sensing, telecommunications, computers, and related technologies have greatly increased the capability for surveillance of people and

¹ Wikipedia entry, <http://en.wikipedia.org/wiki/Surveillance>, accessed 18 May 2006.

their activities. Electronic sensing includes both sensing techniques and techniques for aggregating and comparing computerized records to reveal additional information about an individual. The Fourth Amendment guarantee of 'the right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures' has required, and will in the future require, frequent reexamination and reinterpretation in the context of these new means of surveillance, by both Congress and the Federal Courts. (OTA Report, p12)²

Since 1988, when the OTA report was published, considerable advancement in surveillance technologies has occurred. The OTA report notes that while earlier surveillance technologies

consisted largely of telephone taps and concealed microphones, it now includes many far more sophisticated technologies that can be used to:

1. identify an individual's location or track an individual's movements;
2. monitor and record actions, such as dialing of telephone numbers or automated transactions;
3. listen in on communications or to intercept digital communications;
4. visually monitor behavior; and
5. test or measure reactions and emotions (polygraph testing, voice stress analysis, brain wave analysis, etc.)³

With regard to point 1 above, technologies used to determine an individual's location and track that individual's movements originally involved the monitoring of criminal parolees and probationers by means of electronic transmitter devices such as wrist or ankle bracelets worn by persons whose actions are being monitored.⁴ The term "electronic tagging" is often used here, as noted in the following:

Electronic tagging is a form of non-surreptitious surveillance consisting of an electronic device attached to a person or vehicle, especially certain criminals, allowing their whereabouts to be monitored. In general, devices locate themselves using GPS and report their position back to a control centre, e.g. via the Cellular phone network. This form of criminal sentencing is known under different names in different countries, for example in New Zealand it is referred to as "home detention", and in North America "electronic monitoring" is a more common term.⁵

² U.S. Congress, Office of Technology Assessment, Criminal Justice. "New Technologies and the Constitution." OTA-CIT-366 (Washington, DC: U.S. Government Printing Office, May 1988.)

³ See OTA Report, p 13.

⁴ See OTA Report, p 33-37.

⁵ Wikipedia Encyclopedia internet entry, http://en.wikipedia.org/wiki/Electronic_tagging, accessed 18 May 2006.

Today, available technologies include more sophisticated eavesdropping devices, hidden microphones and cameras, "through the wall" infrared cameras and radar devices, e-mail and fax intercepts, and electronic tracking devices attached to motor vehicles.

2. Remote Neural Monitoring

Available technologies also include remote neural monitoring of individuals. This is done either by using microchips implanted in an individual or through the remote capture of a person's specific electromagnetic "signature." In both cases, remote electronic devices are then used to locate and monitor the activities of the targeted individual.

While precise information on such technology is somewhat limited, there is reason to believe such technologies not only exist, but are being employed, as reported in a document prepared as evidence in a U.S. federal lawsuit against the National Security Administration (NSA) brought about in 1992 by a former NSA employee.⁶ Regarding such the use of this technology in the U.S., it is reported in this document that

The Signals Intelligence mission of the NSA has evolved into a program of decoding EMF waves in the environment for wirelessly tapping into computers and tracking persons with the electrical currents in their bodies. Signals Intelligence is based on the fact that everything in the environment with an electric current in it has a magnetic flux around it which gives off EMF waves. The NSA/DoD has developed proprietary advanced digital equipment which can remotely analyze all objects whether man-made or organic that have electrical activity.⁷

It is further stated in the report that

The NSA has records on all U.S. citizens. The NSA gathers information on U.S. citizens who might be of interest to any of the over 50,000 NSA agents (HUMINT). These agents are authorized by executive order to spy on anyone. The NSA has a permanent National Security Anti-Terrorist surveillance network in place. This surveillance network is completely disguised and hidden from the public.

Tracking individuals in the U.S. is easily and cost-effectively implemented with the NSA's electronic surveillance network. This network (DOMINT) covers the entire U.S., involves tens of thousands of NSA personnel, and tracks millions of persons simultaneously. Cost

⁶ John St. Clair Akwei vs. NSA, Fort Meade, Maryland, filed at the US courthouse in Washington, D.C., February 20, 1992 (Civil Action 92-0449). Mr Akwei claimed to have knowledge of the National Security Agency's structure, national security activities, proprietary technology, and covert operations to monitor individual citizens. The lawsuit was dismissed shortly thereafter in March 1992 for reasons (get)

⁷ John St. Clair Akwei vs. NSA, Fort Meade, Maryland (Civil Action 92-0449).

effective implementation of operations is assured by NSA computer technology designed to minimize operations costs.

NSA personnel serve in Quasi-public positions in their communities and run cover businesses and legitimate businesses that can inform the intelligence community of persons they would want to track. N.S.A. personnel in the community usually have cover identities such as social workers, lawyers and business owners.⁸

It is further stated in the court document that

A subject's bioelectric field can be remotely detected, so subjects can be monitored anywhere they are. With special EMF equipment NSA cryptologists can remotely read evoked potentials (from EEGs). These can be decoded into a person's brain-states and thoughts. The subject is then perfectly monitored from a distance.

NSA personnel can dial up any individual in the country on the Signals Intelligence EMF scanning network and the NSA's computers will then pinpoint and track that person 24 hours-a-day. The NSA can pick out and track anyone in the U.S.⁹

More sophisticated technological capabilities are also described in the court document:

NSA Signals Intelligence uses **EMF Brain Stimulation for Remote Neural Monitoring (RNM)** and **Electronic Brain Link (EBL)**. EMF Brain Stimulation has been in development since the MKUltra program of the early 1950's, which included neurological research into "radiation" (non-ionizing EMF) and bioelectric research and development. The resulting secret technology is categorized at the National Security Archives as "Radiation Intelligence," defined as "information from unintentionally emanated electromagnetic waves in the environment, not including radioactivity or nuclear detonation."

Signals Intelligence implemented and kept this technology secret in the same manner as other electronic warfare programs of the U.S. government. The NSA monitors available information about this technology and withholds scientific research from the public. There are also international intelligence agency agreements to keep this technology secret.

The NSA has proprietary electronic equipment that analyzes electrical activity in humans from a distance. NSA computer-generated brain mapping can continuously monitor all the electrical activity in the brain

⁸ John St. Clair Akwei vs. NSA, Fort Meade, Maryland (Civil Action 92-0449).

⁹ John St. Clair Akwei vs. NSA, Fort Meade, Maryland (Civil Action 92-0449).

continuously. The NSA records and decodes individual brain maps (of hundreds of thousands of persons) for national security purposes.¹⁰

3. Microchip implants

The technology whereby microchips can be implanted in individuals and be used to locate and track their movements is now firmly in place. This technology, sometimes referred to as radio frequency identification (RFID) is described as follows:

Radio Frequency Identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source.¹¹

RFIDs are currently being used in a variety of ways:

Implantable RFID chips designed for animal tagging are now being used in humans as well. An early experiment with RFID implants was conducted by British professor of cybernetics Kevin Warwick, who implanted a chip in his arm in 1998. Applied Digital Solutions proposes their chip's "unique under-the-skin format" as a solution to identity fraud, secure building access, computer access, storage of medical records, anti-kidnapping initiatives and a variety of law-enforcement applications. Combined with sensors to monitor body functions, the Digital Angel device could provide monitoring for patients.¹²

In addition,

Hong Kong Airport imbeds RFID chips in each luggage tag. RFIDs can be more reliably tracked electronically than the old barcode system. Computerized conveyor belt system delivers luggage to the airplanes automatically.¹³

B. Huang Si-ming incident

A front-page article in the January 25, 1996, edition of *The South China Morning Post* reported that an assistant professor at the Hong Kong University of Science and Technology (HKUST) had filed a US\$100 million

¹⁰ John St. Clair Akwei vs. NSA, Fort Meade, Maryland (Civil Action 92-0449).

¹¹ Wikipedia Encyclopedia internet entry, <http://en.wikipedia.org/wiki/RFID>, accessed 18 May 2006.

¹² Wikipedia Encyclopedia internet entry, <http://en.wikipedia.org/wiki/RFID>, accessed 18 May 2006.

¹³ Wikipedia Encyclopedia internet entry, <http://en.wikipedia.org/wiki/RFID>, accessed 18 May 2006.

lawsuit against the U.S. government for implanting a mind-control device in his teeth during a root canal dental procedure. HKUST was also named in the lawsuit on the grounds that it was continuing the mind-control practices initially begun in the U.S.

C. Related matters

The technologies used in passive covert electronic surveillance may also be used for electronic harassment and mind control purposes. For example, the remote neural technology described above may be modified such that electromagnetic energy is directed at target individuals in order to harass them or alter their behavior in some way. Electronic devices used in this manner are sometimes referred to as "non-lethal weapons" and are related to the electronic weaponry being developed and used by military and law enforcement forces. Electronic harassment and mind control practices, which have been reported in the U.S. and elsewhere, not only involve the matter of privacy, they are potentially harmful to the health and well-being of target individuals.¹⁴

III. Issues pertinent to Hong Kong

It would appear that a number of questions are relevant to Legco as it considers legislation related to covert surveillance matters:

1. Are the security agencies and other government agencies in Hong Kong aware of the existence of electronic devices that can capture a person's electronic signature, or that can be implanted in the human body, for the purpose of locating and monitoring from a remote location the activities of that individual?

If no, why not?

If yes, are such devices being used in HK?

If yes, how, where, when and why?

If no, are such devices being considered for future use in Hong Kong?

If yes, under what conditions would the use of such devices be permitted?

2. Would the Hong Kong government permit security and intelligence agencies of other governments to conduct technical surveillance activities within the borders Hong Kong?

If yes, only on their own citizens?

If yes, on citizens other than their own and Hong Kong citizens?

If yes, on Hong Kong citizens?

¹⁴ See, for example, "Electronic Harassment" by Roger Tolces, an electronic security consultant, at www.bugsweeps.com/info/electronic_harassment.html for information about electronic harassment and see, for example, the Radiation Health Foundation, Inc. website www.rhfweb.com for information about electronic harassment and mind control.