Session 20

Enforcement Agencies' Power of Surveillance: The Need for Governance

By

Abdul Samad Abdul Ghani
Lecturer, Faculty of Law
University of MalayA

ENFORCEMENT AGENCIES' POWERS OF SURVEILLANCE: THE NEED FOR GOVERNANCE

Abdul Samad Abdul Ghani
Faculty of Law
University of Malaya, Kuala Lumpur.

The use of surveillance for purposes of crime prevention and detection as well as investigation and prosecution of crime has important benefits to society. The rise of urbanisation, technological growth and increase in information, capital and human movement as a result of globalisation, state surveillance or intelligence activity are increasingly perceived as an important tool to deal with the threat of organised crime and international terrorism. However, the use of surveillance by enforcement agencies can be regarded as an exercise of overwhelming state power. As the use of surveillance is necessarily secretive and hidden, it creates an imbalance in power relation between the state and the people that it govern. Such a condition of imbalance make the practice of surveillance vulnerable to abuse or misuse which may affect not only the integrity of the state in the eyes of its citizen but also the ethical standing of law enforcement bodies. The use of surveillance also creates significant risk to individuals' privacy and autonomy. If such use is pervasive enough, surveillance may inhibit society and limit its ability to generate ideas and progressive thoughts. Consequently, enforcement bodies power of surveillance need to be subjected to a high degree of control in terms of legal and democratic accountability. Various democratic mechanisms and regulatory framework need to be put in place to ensure that the use of surveillance is accounted for and not abused. It must also be admitted that the control of surveillance by state bodies are not without debate. Often, the debate revolves around the degree and nature of control that must be imposed upon the exercise of surveillance. However, it remain the case that the overwhelming risk posed by the state power of surveillance should nto persist without democratic and legal control.

The paper has a very limited aim: to look at the laws in Malaysia that provides for the powers of surveillance and consider whether there are in place sufficient legal and non-

legal controls over the power of surveillance of enforcement bodies in Malaysia. If it is found that some forms of improvement are necessary, the paper will offer suggestions for the future governance of surveillance practice by enforcement bodies in Malaysia. Reference will be made to the laws in the United Kingdom - primarily the Regulation of Investigatory Powers Act 2000 - to provide some comparison.

A. Backgrounds to the Laws and Practice of Surveillance in Malaysia

A discussion on the laws and practice of surveillance in Malaysia has to be based on some legal-political backgrounds. These backgrounds could provide some degree of explanation as to the nature of the laws that govern or provide for surveillance in Malaysia. The need for governance of state surveillance activities can be discussed in the light of two critical backgrounds:

1. an absent of a right to privacy

(i) The Federal Constitution does not recognised privacy as one of its fundamental rights. In *PP v Hj Kassim* [1971] 2 MLJ 115, the Federal Court was asked to consider whether article 5 of the Federal Constitution regarding the right to life and liberty can be extended to include the notion of privacy. If that was the case, the trial judge could not allow a confidential communication between a patient and his psychiatrist to be admitted in evidence. The Federal Court instead held that the trial judge had to adhere to the provisions in the Evidence Act 1950 which provided that, when a fact is admissible, a trial judge is under a duty to receive it unless it can be excluded as provided by sections 24 and 25. The Federal Court however, did not take the opportunity to consider the possibility of such an extension to the meaning of the right to life and liberty under article 5.

(ii) In the case of *Ultra Dimension Sdn Bhd v Kook Wei Kuan*[1] the High Court of Kuala Lumpur held that there is no right to privacy under the common law in Malaysia and that there is no tort of invasion of privacy, referring to the English decision of *Kaye v Robertson* [2]

(iii) The proposed data protection regime under the Personal Data Protection Act has never materialised. The proposal was conveyed to the public in 2000 as part of the Multimedia Super Corridor (MSC) cyberlaws. Such a data protection regime could

---

1 2001 MLJU LEXIS 793; [2001] 751 MLJU 1

2 (1991) FSR 62

protect the information privacy of Malaysians and limit how the government collect and handle personal data.

2. Rigorous use of enforcement powers for purposes of protecting national security and public order.

(i) Various proclamations of emergency, including that of 1969, are still in operation and provide justification for laws and criminal enforcement practice that are focussed on preventing and curtailing threats to national security and public order.

(ii) Security legislations like the Internal Security Act 1960 and ESCAR 1975[3] have been rigorously applied, initially to tackle the threat from communist insurgent and lately, alleged Al-Qaeda-linked terrorist groups like Jamaah Islamiah and Kumpulan Militan Mujahidin. However, the ISA 1960 has received criticisms for its application against lesser threats.[4]

(iii) The use of security laws and state powers on the ground of protecting national security and public order could be a dominant influence in the use of powers of surveillance. Such justifications could also hinder further governance of surveillance.

B. Powers of Surveillance under Malaysian Laws

Malaysia does not have an omnibus laws that govern various aspects of surveillance powers like the United Kingdom Regulation of Investigatory Powers Act 2000. However, there are statutory provisions that provide for powers of surveillance whether directly or indirectly. On the other hand there is a large area of surveillance practices that are in need of legislative control. This paper will focus on two aspects of surveillance that have some degree of statutory basis: interception of communication and data surveillance.

1. Interception of Communication

Interception of communication often refers to the interception of telephone, electronic or radio communication. A common example of interception of communications is telephone tapping. Section 6 of Communication and Multimedia Act 1998 (or CMA 1998) could provide some assistance:

---

[3] Essential (Security Cases) (Amendment) Regulations 197 (P.U.(A) 362)

[4] for example, see the Federal Court decision in *Mohamad Ezam Bin Mohd Noor v Ketua Polis Negara & Other Appeals* [202] 4 MLJ 449

"communications" means any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms;

"intercept" means the aural or other acquisition of the contents of any communications through the use of any electronic, mechanical, or other equipment, device or apparatus;

However, a wider notion of interception of communications would include intrusion into correspondence in the form of interception of postal articles. It may also include the recording of real conversation using covert listening device. The discussion the will focus on the interception of communication in the sense of section 6 of the CMA 1998 as well as interception of postal articles. There is no law in Malaysia that govern the use of covert listening device or similar forms of technical surveillance.

Prohibition against interception of communications

In general, the CMA 1998 section 234(1), criminalise interception of communications and disclosure of the content of any communication, unless the interception and disclosure is made with lawful authority under the CMA 1998 or any other written law. Section 234 (1) even make it an offence to use or attempt to use the content of any communications that has been obtained through unlawful interception. The power to prosecute for offences under the CMA 1998 is in the hand of the Public Prosecutor since his written consent is required before any prosecution can be instituted.[5]

Lawful interception of communications

(i) power to intercept communication in relation to investigation into specific type of offences.

A number of statutory provisions provided for interception of communications in relation to specific type of offences. These provisions are:

(a) Communication and Multimedia Act 1998, section 252,
(b) Anti-Corruption Act 1997, section 39,
(c) Dangerous Drugs (Amendment) Act 1983, section 27A,
(d) Dangerous Drugs (Forfeiture Of Property) Act 1988, section 20, and
(e) Kidnapping Act 1961 (Revised 1989), section 11.

---

[5] (section 259)

As an example, section 252 of the Communication and Multimedia Act 1998 provides the Malaysian Communication and Multimedia Commission (or any 'authorised officer') with the power to intercept communication in relation to an investigation into an offence under the CMA 1998 or its subsidiary legislations.

In addition to the provisions above the recent amendment to the Criminal Procedure Code provides for the interception of communications to deal with terrorism. According to section 9 of the Criminal Procedure Code (Amended) 2006 (Act A1274),[6] the amended Criminal Procedure Code will now include a specific provision that empower the Public Prosecutor to authorise interception of communications to deal with terrorism offences. The provision also empowers the Public Prosecutor to authorised interception of postal articles. Under the soon-to-be-added section 106c(1) Criminal Procedure Code,

> notwithstanding any written law, the Public Prosecutor, if he considers that it is likely to contain any information relating to the commission of a terrorism offence, may authorize any police officer
>
> (a) to intercept, detain and open any postal article in the course of transmission by post;
> (b) to intercept any message transmitted or received by any telecommunication; or
> (c) to intercept or listen to any conversation by telecommunication.

According to the amended section 106A, "terrorism offence" means a terrorist act or a terrorism financing offence. However, the amended Criminal Procedure Code does not provide further definition to these terms. Instead, the amended section 130B(2), Chapter VI A of the Penal Code[7] provide a list of broad and expansive definitions of a 'terrorist act' which include 'act or threat of action ...that ...involves prejudice to national security or public safety'.

The powers to intercept communication under these provisions suffer from very serious lack of accountability and scrutiny particularly at the point of the authorisation of an interception. Specifically, the problems are as follows:

---

[6] the statute received the Royal Assent on 27 September 2006 and was gazetted on 5 October, 2006, the amendments are not yet enforced.

[7] Yet to be in force.

(a) The primary problem with the above provisions is the granting of unaccountable and unguided power to the Public Prosecutor to authorise interception of communications.

(b) There is clearly no prior scrutiny by a judge before an interception can be authorised because no judicial warrant is required for an interception. Only the Public Prosecutor is empowered to authorised interception.

(c) In contrast, various statutes that provide powers of investigation to enforcement bodies, including the CMA 1998[8] requires a search warrant to be authorised by a Magistrate before a search can be conducted on any premises. The American approach, for example, is to draw a parallel between interception of communications with search and consider it unlawful for an interception of communication to be conducted without a judicial warrant.[9]

(d) These provisions above do not require strenuous justifications before interception can be authorised. Basically, the Public Prosecutor may authorise an interception if he considers that such a method could yield information that could provide evidence into the offence in question. Although, an authorisation of interception of communications under the amended section 106c(1) Criminal Procedure Code will require

(e) In comparison to the provision under the United Kingdom Regulation of Investigatory Powers Act 2000, there is no requirement that the Public Prosecutor must be show that the use of interception of communications is 'proportionate' to what it seek to achieve. [10] This may result in indiscriminate and even excessive use of interception of communications for investigating those offences. The use of interception of communication could be disproportionate to the intrusion of privacy that it may caused and therefore, other means of investigation should be considered and exhausted. In contrast, the Regulation of Investigatory Powers Act 2000 provides that the Interception of Communications Code of Practice[11] that must be followed before a warrant can be authorised.

(f) The provisions under the Malaysia statutes does not require the Public Prosecutor to specify any condition or time limit on the authorised interception of communications. On the other hand, a warrant would not simply act as a judicial approval for the interception; it could specify detail requirements and conditions including information as to the specific method to be use and the duration of the

---

8 section 252

9 see *Katz v US* (1967) 389 US 374

10 See Cousens,M., (2004) *Surveillance Law*. pp.133-134

11 SI 2002/1693. Available at <URL:http://www.hmso.gov.uk/si/si2002/20021693.htm> [Accessed 10 March 2005]

operation. Again, these requirements are practically useless unless there is an independent supervisory body to scrutinise and hold the practice accountable.

The CMA 1998 section 252 can also be criticised for giving disproportionate power to use interception of communications in relation to various types of offences that are covered by the Act. Most of these offences are not 'serious offences' because CMA 1998 is fundamentally legislated to regulate convergence of media as well as supporting the growth of the ICT industry in Malaysia. Only a number of offences that relates to disruption or abuse of communication networks (such as in sections 231 to 235) may justify some use of interception of communications. Clearly, section 252 ought to be more specific as to the nature of offences that justifies the use of interception on communications.

(ii) Interception of Communications under Special Powers in Emergency

Enforcement bodies, especially the police, are enabled with a more general and expansive power to intercept communication for reasons of emergency and national security.

(a) interception of communications for purposes of tackling public emergency or in the interest of public safety under the CMA 1998.

The CMA 1998 section 266(1) (c) provides that on the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong[12] (or the Minister authorised by him) may order for interception of communications. The CMA 1998 does not define 'public emergency,' but the meaning could be reflected against the power of the Yang di-Pertuan Agong to proclaim emergency under Article 150 of the Federal Constitution in expectation of or under actual 'grave emergency...whereby the security, or the economic life, or public order in the Federation or any part there of is threatened.'

---

12 The Yang di-Pertuan Agong is the Supreme Head of the Federation of Malaysia (article 32 of the Federal Constitution). Though, as a constitutional monarchy, article 40 of the Federal Constitution requires the Royal Highness to exercise his constitutional and statutory power according to the advice of the Cabinet (except in very limited and notional circumstances as provided by the Federal Constitution).

(b) interception of communications under ESCAR 1975[13]

Under the Essential (Security Cases) (Amendment) Regulations 197 (P.U.(A) 362) regulation 23 (1),

> The Public Prosecutor may, if he considers that any articles or message sent through the post or telecommunications are likely to contain any information relating to a security offence, authorise any police officer either orally or in writing
>
> (a) to intercept, detain and open any postal article in course of transmission by post;
> (b) to intercept any message transmitted or received by any telecommunication; or
> (c) to intercept or listen to any conversation by telephone.

This power to intercept communications under ESCAR is only exercisable in relation to a 'security offence' which is define in regulation 2 as an offence against section 57,58, 59, 60, 61 or 62 of the Internal Security Act. But it could also includes statutory offences the commission of which is certified by the Attorney-General as affecting the security of the Federation. The nature of offences that are covered under section 57,58, 59 of the ISA 1960 are offences connected to the carrying, possession, supplying and receiving of firearms, ammunition or explosives[14], while section 60 ISA1960 relates to any failure to report those offences. Sections 61 and 62 relates to attempts to commit those offences and assisting a person who has committed those offences.

(c) interception of postal communications under the Postal Services Act 1991

According to section 7(1) of the Postal Services Act 1991, the Yang Di pertuan Agong may authorised the Malaysian Communications and Multimedia Commission (or any other authorised government officer) to intercept and disclose the content of 'any postal article or class of postal articles' - 'on the occurrence of any industrial unrest, strike, lockout or any other event which gives rise to an emergency, or in the interest of national or public security'

---

13 ESCAR 1975 was originally an emergency regulation made under section 2 of the Emergency (Essential Powers) Ordinance No.1, 1969 which is now replaced by Emergency (Essential Powers) Act 1979 Act 216. ESCAR 1975 is a subsidiary legislation made under an ordinance promulgated by the Yang di-Pertuan Agong, in the exercise of his power under Article 150 of the Federal Constitution, in relation to the 1969 Proclamation of Emergency.

14 see Appendix II.

The power of interception of communications under the CMA 1998 section 266(1) (c), ESCAR 1975 regulation 23, and Postal Services Act 1991 section 7(1) - which deal with states of emergency as well as threats to security and public order - can be criticised for a number of reasons.

(i) The provisions are expansive in that they may allow interception of communications on the ground of protecting security and public order. ESCAR 1975 permits the use of interception of communications on other offences that have been certified by the Attorney-General[15] as 'affecting the security' of the country. Consequently, ESCAR 1975 bestows the Attorney-General with unlimited power to certify any offences as a 'security offence and then acted as the Public Prosecutor to authorise a police officer or conduct interception of communications in relation to those offences.

(ii) The authorisation and exercise of interception of communications under the provisions lack judicial and legislative scrutiny, accountability and control.

(iii) Beside similar criticisms above as to the overt power of the Public Prosecutor under regulation 23 of ESCAR 1975, it is clear that interception of communications for purposes of dealing with threat to security and public order can be applied limitlessly as the provisions have entrusted the Executive to make decision without proper accountability and scrutiny. As an example, section 7(4) of the Postal Services Act and section 266(1) of CMA 1998 does not require detail explanation for the use of interception of communications. Hypothetically, these two provisions could allow a disproportionate and persistent use of surveillance over an unspecified period of time.

Presumably, the exercise of the power to intercept communications these provisions are to be utilised in the face of impending or ongoing state of emergency; but the facts that these statutes have endowed complete discretion of the Executive is a matter of grave concern fundamentally the lack of formal legislative or judicial scrutiny could result in arbitrary and pervasive use of interception of communications.[16] The requirement for communication and network service providers to make ready interception of communications facilities under the section 265 (1) the CMA 1998 further illustrate the desire maintain the power of surveillance.

---

15 Under article 145 of the Federal Constitution, the Attorney-General is appointed by the Yang di-Pertuan Agong, apparently under the advice of the Cabinet.

16 see for discussions on the position of emergency laws in relation to the Constitution see, Lee.H.P. (1995) *Constitutional Conflicts in Contemporary Malaysia* (Oxford, Oxford University Press)

2. Data surveillance

Law enforcement requires access to data for purposes of preventing, detecting and prosecuting crime. This data provide what is known as criminal intelligence information and may not always be used for purposes of criminal evidence. Criminal intelligence information may be amalgamated from various sources: publicly available information, third parties data holder and direct surveillance(data in the form of photos and audio recordings). The advent of computerisation provide legal enforcement bodies with possible access to disparate computer databases. Computerisation too could enable enforcement bodies to gather, store and process large amount of data. Extensive data search and process can be supported by technologies of data mining and data matching which may help enforcement bodies to generate profiles of suspects or criminals.

Data surveillance may involve covert and non-consensual gathering of data and could target individual persons as well as non-human entities like organisations or corporations. The nature of data that is gathered may range from individual private information to confidential business information. Covert and non-consensual access to data create serious problem to private bodies in terms of loss of confidentiality and control over their business information. So far, there is little recognition of private non-human entities right to information privacy as it is difficult to draw such a parallel to human demand for privacy. However, there are concerns that data surveillance might be abused for purposes of economic espionage or even blackmailing .

This discussion, however, will focus on the impact of undisclosed access to and secret gathering of personal data from the perspective of individual desire to information privacy.[17] The notion of information privacy can be described as an individual's right to control access to his/her personal information and his/her right to control how others handle his/her information. An infringement of information privacy therefore includes direct informational intrusion as well as abuse of personal information in the hand of third parties. In general, concerns about data surveillance from the perspective of information privacy revolve around these aspects:

i. surreptitious or non-consensual collection of personal data whether directly of from third parties;
ii. the accumulation of personal data in law enforcement database; and

---

17

iii. the handling of those data especially in terms of their sharing, accuracy and ultimate disposal.

Hence, the practice of data surveillance need to be govern from the following perspective:

i. the power to access personal information, albeit surreptitiously and often in the hand of a third party, must be based on clear laws;

ii. the law must provide for prior authorisation as well as external modes of scrutiny and accountability;

iii. access to data must be based on legitimate grounds and govern by the requirement of necessity and proportionality;

iv. the actual gathering, storing and handling of the data must be transparent for purposes of accountability and scrutiny by a relevant supervisory body.

v. the data in the possession or control of an enforcement body must be handle according to data protection or fair information principles, without jeorpadising investigation, national security and public order.

Laws empowering access to data

Laws that provide for investigatory powers naturally provide relevant enforcement bodies with the power of search in order to gather information and data for purposes of investigation. There are various statutory provisions which provide for the power of search as well as the power to compel production of or give access to information. Key concerns about such legal powers revolve around the potential for abuse of those data, particularly if they are used for purposes unrelated to the investigation such as the gathering of intelligence information. It is necessary to look at some of the provision ad consider among all whether there are sufficient safeguards in place.

There is no compelling constitutional duty to conduct search with a warrant. Although the Criminal Procedure Code provides for the power of search (of person and premises) with a judicial warrant, it permits search without a warrant under 'urgent' circumstances such as where an application of a warrant could hamper an impending access to evidence. Specific criminal statutes and statute that empowers enforcement bodies also provide specific powers of search, often allowing search without warrants. The power to search premises may enable the relevant enforcement officers to gather evidence that may help in the investigation and/or prosecution of a crime. However, a number of statutes has given powers to enforcement bodies to access data in computers that are obtained during the search. Two of the most critical legislations are the

Computer Crimes Act 1997 and the CMA 1998 which provides for access to computer data.

Section 10 Computer Crimes Act 1997 [18] (or CCA 1997) provides for the search of premises by a warrant from a Magistrate (or without one if there is an urgency - believe that warrant will frustrate investigation) where the police has reasonable cause to suspect that there is evidence of a commission of offence under the CCA 1997. The provision is wide enough to enable the police to access computer files or data regardless of whether they are in the hand of a suspect.[19] This might include cases where the data are in the possession of an internet service provider or even in the server of a web hosting company. In addition, section 10(1) (b) empowers the police to compel a person who has control or access to the computer (in terms of security access codes and encryption) to provide assistance.[20]

Similar power can also be found in **section 249 of the CMA 1998.** Under that provision, a police officer conducting a search of premises (for the purpose of enforcing the CMA 1998) either with a warrant (section 247) or without a warrant (section 248) can compel access 'to computerised data whether stored in a computer or otherwise'. This provision is even wider than the CCA1997 because the police officer can require for the provision of 'necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data' to access the data in the computer. In addition, he may also gain 'access' to the data by making copies of the data stored in the computer.

However, and anomalously enough, there is no requirement for a warrant before an 'authorise officer' (which normally mean an officer of the Malaysian Communication Multimedia Commission) can have access to computerised data.According to **section 254 CMA 1998,**

> An authorised officer shall, for the purposes of the execution of this Act or its subsidiary legislation, have power to do all or any of the following:

---

[18] The Computer Crimes Act 1997 basically provide for the criminalisation of illegal access to computer (include computer hacking, and other non-consensual access to computer) and computer attacks.

[19] *a)* have access to any program or data held in any computer, or have access to, inspect or check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act;

[20] (section 11 - non-compliance with the demand is an offence punishable by a max fine twenty-five thousand ringgit or to imprisonment for a term not exceeding three years or to both.)

(a) to require the production of records, accounts, computerised data and documents kept by a licensee or other person and to inspect, examine and to download from them, make copies of them or take extracts from them;

An even wider power to access data can be found in **section 73 of the CMA 1998.** the Commission may compel any person to provide information 'whether in physical form or electronic media' 'if the Commission has reason to believe that the person ...has any information (including but not limited to accounts and records) or any document that is relevant to the performance of the Commission's powers and functions under this Act or its subsidiary legislation'.

The primary concern in relation to the exercise of this power of access to information is that the CMA 1998 give broad powers to the Commission (an 'authorise officer) to administer the statutory powers and to prosecute a wide range of offences under the Act. The CMA provide specific powers of enforcement like section 233 which make it an offence to use computer network (for example, the Internet) 'to make, creates or solicits; and initiates transmission... of any comment, request, suggestion or other communication which is obscene, indecent false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person...'; as well as broad powers such as that under section 266 ' special powers in emergency.' Although the preamble to the CMA 1998 state that it is, 'An Act to provide for and regulate the converging communications and multimedia industries, and for incidental matters', section 3 of the Act contemplate the application of the statutory powers for purposes of ensuring 'information security and network reliability and integrity.' It seems that the Commission is expected to 'police' of communication activities in Malaysia, particularly in reflection of Government constant resort to the Commission to assist in 'identifying' writers of libellous or seditious e-mails.

There are various other statutory provisions which grant enforcement bodies with wide powers to access data and information in the hand of a suspect or a third party who may have relevant information.[21] These provisions including those discussed immediately above, are clearly inadequate as far the protection of individual information privacy is concerned. Section 73 and section 254 of the CMA 1998 provide powers of access to

---

[21] Anti-Money Laundering Act 2001 Part IV, Official Secrets Act 1972 Section 20, Customs Act 1967 (Revised - 1980) Section 111b, and Anti Corruption Act Section 28.

information without even the need for an authorisation by a judicial warrant. This could result in the abuse of the power to access information unrelated to the actual purpose of the provisions. In addition, the power of access to computer or computerised data is of great concern because it enable unregulated and unaccountable access to data which are secondary or unrelated to the investigation. Once these data are in the hand of the enforcement body concern they may deal with the data in an unaccountable fashion - largely because there is no regulation or no code of conduct that govern their action once the data is in their possession (except perhaps, to a limited extent, the Official Secrets Act 1972). In this manner, data obtained from the exercise of powers of search or powers to compel disclosure of information as well as the powers themselves may be use for purposes of surveillance.

Clearly, there is a need for further safeguards in terms of guidance on the handling of the data obtained under these powers. In addition some form of scrutiny whether judicial, legislative or institutional may be necessary to ensure that data are not collected for surreptitious purposes, or if that is the case, that stringent controls are put in place to prevent abuse. Beyond improving the relevant statutes, further legislative and policy approach may be necessary to prevent abuse and to improve the protection of information privacy.

Data practice and enforcement bodies

An extension of the issues above is the issue of governing personal data in the hand of enforcement bodies (and even government). Other than the Official Secrets Act 1972 which govern government classified information, there is no legislation that govern data practice by government bodies. One approach is to enact statutes that govern how public authorities are suppose to handle personal data. Such statutory approach can be found in the American Privacy Act 1974, the Canadian Privacy Act, and the United Kingdom Data Protection Act 1998. The data protection principles under the United Kingdom data protection regime (which to some extent, similar to the fair information principles under the American and Canadian laws) would require, among all, that individuals must be informed of the purpose of which their data are being collected; that measures are taken to ensure the security, integrity and accuracy of the data; and that individuals are given access to their data either for the purpose of knowing about their existence in the hand of the data controller or for determining the accuracy of their data.

In addition, a data protection regime would also requires that a government bodies do not use the data under their control for purposes other than for which they are

collected. More importantly, an enforcement body would be required under a data protection regime to be transparent as to how it collect, keep, use and dispose personal data. In any case, a data protection would provide some degree of exemption where data have been collected or used for purposes of criminal investigation or national security. But this limitations are only in regards to access to such information individuals. On the other hand, an internal supervisory bodies could be appointed to oversee the use of personal data by enforcement bodies in order to ensure accountability and prevent abuse. To date however, Malaysia does not have any law that govern the collection and handling of personal data. The government has planned to introduced a data protection legislation and a specific statute on electronic government but there has been very little progress in this area. In addition, freedom of information laws could be legislated to ensure public access to their information in the hand of the government. But in the light of the persistence use of the Official Secrets Act, a freedom of information legislation could remain a distant aspiration.

C. Surveillance in Malaysia: The Need for Governance

The previous discussions show that statutory provisions that attempt to govern or provide for powers of surveillance have serious deficiencies in many aspects. It appears that there has been minimal legislative effort to control the exercise of the powers of surveillance by enforcement bodies in Malaysia. In fact, there are various forms of surveillance methods that are yet to be regulated by laws. As already mentioned above, there is no legislation to regulate the use of covert listening or photographic devices to intrude into individual privacy. The growing dependence on CCTV, both as a tool of crime prevention and surveillance, would require statutory controls or risk intrusion of privacy and abuse of video images.[22] The use of covert human surveillance such as informers and undercover infiltration would also require legislation. A number of statutes[23] has provided for the protection of informers which insulate them from being scrutinise in the court. The practice of covert human surveillance need to be regulated in areas such as the payment of informants and the use of child informants.

In addition to improving existing laws and introducing new legislations, there is an urgent need to create an independent supervisory body to oversee and scrutinise the practice of surveillance by enforcement bodies. For example, under the United Kingdom

---

[22] See for example the United Kingdom Information Commissioner *CCTV Code of Practice*. 2000.
[23] Section 5, Anti-Money Laundering Act 2001; Section 53, Anti-Corruption Act 1997. Section 124A Customs Act

Regulation of Investigatory Powers Act 2000 three bodies are responsible for the monitoring and review of surveillance activities: Interception of Communications Commissioner, Office of Surveillance Commissioners and (OSC) Intelligence Services Commissioner. Such a supervisory body could scrutinise decisions to authorised surveillance whether made under a warrant or otherwise. The role of such an independent supervisory body[24] is not simply about monitoring compliance to related legislative powers, but also to support systemic or operational changes. In addition, such an independent body could be required to regularly report to the legislature and the public so that the depth and extent of surveillance in this country can be known. Based on such reports, the legislature, if it is responsive enough, could question the relevant Ministers about the surveillance practice of enforcement bodies under their responsibility.

More importantly, a system of sanction and remedy delivery would also be required so that surveillance abuse can be discouraged. Under the United Kingdom Regulation of Investigatory Powers Act 2000, an Investigatory Powers Tribunal functions to provides an independent judicial oversight by receiving complaints from aggrieved members of public. Such a body could make decisions in ways that balance the collective need for security and public order against the interest of individual in their privacy. However, it is important that such an adjudicative body is empowered to sanction surveillance abuse and is given the power to punish specific individuals.

Conclusion

This paper has only covered a small aspects of the power of enforcement bodies to use surveillance. Nonetheless, it shows that there are serious issues that need to be dealt with in relation to these powers. Exercise of the powers of surveillance in Malaysia need to be subjected to concrete judicial and democratic control. In the light of increasing availability of sophisticated surveillance technologies and the desire to maintain security and safety of the nation, the urge to monitor, observe and track citizens need to be tempered with a high degree of scrutiny and accountability. Control of powers of surveillance is necessary in the interest of protecting human rights, democratic values and the rule of law.

[24] For example, part V of the RIPA 2000 requires the appointment of a judge to be the Interception of Communications Commissioner

References:

Akdeniz, Y, and Walker, C., (2000) 'Whisper Who Dares: Encryption, Privacy Rights And The New World Disorder', in Akdeniz, Y, Walker, C., Wall, D., eds., (2000). *The Internet Law and Society*. Harrow: Pearson Education.

Akdeniz, Y. et al., 'Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals', 1997 (2) *The Journal of Information, Law and Technology (JILT)* (online). Available at: <URL: http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/> (Accessed 18 October 2003).

Akdeniz, Y., 'UK Government Encryption Policy', (1997) Web Journal of Current Legal Issues 1 (February) at <http://www.ncl.ac.uk/~nlawwww/1997/issue1/akdeniz1.html>.

Azmi, I. M., 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill', *17th BILETA Annual Conference*, 5-6 April, 2002, Free University, Amsterdam.

Bingham, T., 'Opinion: Should There Be a Law to Protect Rights of Personal Privacy', (1996) *5 European Human Rights Law Review 450*.

Bloustein, J., 'Privacy as an Aspect of Human Dignity', (1964) *39 New York University Law Journal 962*.

Christie, K. and Roy, D., (2001) *The Politics of Human Rights in East Asia*. London: Pluto Press.

Colvin, M., (2002) *Developing Key Privacy Rights*. Oxford: Hart Publication.

Cousens, M., (2004) *Surveillance Law*. London: LexisNexis-Butterworth.

Ferguson, G. and Wadham. J., 'Privacy and Surveillance: A Review of The Regulation of The Investigatory Powers Act 2000', (2003) *European Human Rights Law Review* (Special Issue: Privacy), p.101-108.

Home Office. The Interception of Communications in the United Kingdom (Cmnd.9438, 1985). London: HMSO.

JUSTICE, (1998) *Under Surveillance: Covert Policing and Human Rights Standards*. London: Justice.

Khaw Lake Tee, Towards a Personal Data Protection Regime in Malaysia. *Journal of Malaysian and Comparative Law*. Vol.29 (2002) 255

Lyon, D., (2000) *Surveillance Society*. Cambridge, Polity Press.

SUARAM (2004) *Malaysia: Human Rights Report 2003 - Civil and Political Rights*. Petaling Jaya, Selangor: SUARAM.

Walker,C. P., 'Police Surveillance by Technical Devices' (1980) Public Law 184;

Walker, C. P. and Akdeniz, Y., 'Anti-Terrorism Laws and Data Retention: War is Over?' (2003) *Northern Ireland Legal Quarterly*, Vol. 54, No. 2, Summer Edition, p.159-182.