WORKPLACE PRIVACY IN MALAYSIA: A LEGAL COMPARISON

Zainal Amin Ayub
Zuryati Mohamed Yusoff

The rapid growth of the information and communication technology has made it possible for everyone to search information, gain knowledge, and generate efficiency in their work in such a way that we never dreamed of a decade ago. Another shift has occurred in the digital world where it reflects a growing interest in new surveillance technologies, be it relating to personal or company's data. This interest is based on various reasons; it enables the companies to monitor work performance, maintain employees' discipline and productivity, and introduce e-commerce transaction in the company. Those new technologies include video surveillance, smart card, face recognition, and biometrics. Many countries are also developing new identification and authentication systems, such as smart cards and digital identification cards. Austria is promoting a new social security smart card; Singapore also created "SingPass" and Malaysia has established "Mykad", a universal purpose ID card. These collections of data have significant importance regarding the issues of its security and individual privacy. Furthermore, the Malaysian Federal Constitution does not specifically recognise privacy as one of the fundamental rights and the Personal Data Protection Bill is yet to be enforced. As such, this paper will discuss the extent of protection available to the workers relating to their privacy under related laws in Malaysia.

PRIVACY DEFINED

Definitions of privacy vary widely according to context and environment, and in many countries the concept has been fused with data protection, which interprets privacy in terms of management of personal information. Protection of privacy is basically the limit at how far society can intrude into a person's affairs. In the 1890s, United States Supreme Court Justice Louis Brandeis (Wasren & Bandeis, 1980) articulated a concept of privacy that urged that it was the individual's right to be left alone. Brandeis argued that privacy was the most cherished of freedoms in a democracy, and he was concerned that it should be reflected in the Constitution. According to Bloustein (1964), privacy is an interest of the human personality. It protects the inviolate personality, the

individual's independence, dignity and integrity. Smith (2000) defined privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."

Privacy is the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when the disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities (Standler, 1997). The right of privacy is restricted to individuals who are in a place that a person would reasonably expect to be private for example in home, hotel room, telephone booth, etc. There is no protection for information that either is a matter of public record or when the victim voluntarily discloses it in a public place. People should be protected by privacy when they believe that the conversation is private and cannot be heard by others who are acting in a lawful manner (Standler, 1997).

The right to privacy has been expressed as a fundamental human right. Article 12 of the UN Universal Declaration of Human Rights adopted in 1948, proclaims that: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor and reputation. Everyone has the right to the protection of law against such interference or attacks". However, the Federal Constitution of Malaysia does not specifically recognise the right to privacy, but does provide for several related rights, including freedom of assembly, speech, and association. Whilst freedom of movement is protected in article 9 of Federal Constitution, it, however, states that: (1) No citizen shall be banished or excluded from the Federation, (2) Subject to Clause (3) and to any law relating to the security of the Federation or any part thereof, public order, public health, or the punishment of offenders, every citizen has the right to move freely throughout the Federation and to reside in any part thereof and (3) So long as under this Constitution any other State is in a special position as compared with the States of Malaya, Parliament may by law impose restrictions, as between that State and other States, on the rights conferred by Clause (2) in respect of movement and residence.

Further, article 10 of the Federal Constitution provides: Subject to Clause (2), (3) and (4), (a) every citizen has the right to freedom of speech and expression; (b) all citizens have the right to assemble peaceably and without arms; and (c) all citizens have the right to form associations.

However, certain restrictions regarding the above rights may be imposed by the law in order to safeguard the interest and security of the Federation and to maintain public order. In other words, rights granted under Article 10 are not absolute. There are laws limiting the rights protected in Article 10, those laws to clarify the position in Malaysia regarding freedom of speech and expression which is actually a limitation on the law of privacy for example the Official Secrets Act 1972 as opposed to the rights of disclosure of public servants. This

is more for protecting government privacy rather than employees. Other related statutes also limit the rights of individual privacy, for instance, section 39 of the Anti-Corruption Act 1997, section 245 up to section 247 of Communication and Multimedia Act 1998, section 30 of Internal Security Act 1960, section 10(2) and (3) Computer Crimes Act 1997, and Anti Money Laundering Act 2000. These provisions showed that rights to privacy are recognised but limited in its application.

PRIVACY AT THE WORKPLACE: AN INTRODUCTION

Employees around the world are normally subjected to some kind of monitoring by their employers. For various reasons, employers collect personal information from employees, such as health care, tax, and background checks. Traditionally, this monitoring and information gathering in the workplace involved some form of human intervention and either the consent, or at least the knowledge, of employees. The changing structure and nature of the workplace, however, has led to more invasive and often, covert, monitoring practices which call into question employees' most basic right to privacy and dignity within the workplace. Progress in technology has facilitated an increasing level of automated surveillance. Now, the supervision of employee performance, behaviour, and communications can be carried out by technological means, with increased ease and efficiency. The technology currently being developed is extremely powerful and can extend to every aspect of a worker's life. Software programs can record keystrokes on computers and monitor exact screen images, telephone management systems can analyse the pattern of telephone use and the destination of calls, and miniature cameras and *Smart* ID card can monitor an employee's behaviour, movement, and even physical orientation.

The usage of the Internet, the numerous websites and e-mails has contributed to the efficiency and excellence in business. These tools are relatively cheap, quick, and an easy form of communication. However, the availability of e-mail and other form of communication technologies posted considerable opportunities for misuse. For instance, a study by Girald (1997) suggests that more than 30% of all email messages sent by employees are non work related. Similarly, the IDC Research survey 1999 reported that 30-40% of Internet access within the corporate workplace is not business related (Draycott, 2000). However, the recent self-report Elron study 2000 (Draycott, 2000) of corporate Internet usage revealed a more alarming figure. Out of 576 respondents who have access to the Internet and e-mail at work, more than 85% of them had used these facilities for personal matters. Secure Computing survey 2000 confirmed these findings of non-work related use of the Internet and e-mail, when they reported that 50% visited pornographic sites, 92% bought goods online, 84% searched for jobs online, and 54% visited chat rooms whilst at work (Hamin, 2001).

EMPLOYER-EMPLOYEE RELATIONSHIP

The doctrine of vicarious liability applies to all forms of torts. The employer will be exposed to legal risk of potential civil claims for example contract, tort of negligence, defamation, sexual harassment, or potential criminal actions for publication of obscene materials. Many reasons have been put forward in justification of this doctrine, some of which are that a master is to be held liable for employing a negligent employee; for failure to control the employee. Since the master derives benefit from the employee's work, he should be made liable for any tortious conduct of the employee in the performance of his work. Another reason is because the master is in a better financial standing to compensate the third party. This last reason ensures, if nothing else, that the third party will in fact receive compensation for his injuries and the doctrine therefore secures actual compensation to the tort victim (Talib, 2003).

The general basis for the liability of employers for the conduct of employees may be drawn from the principle of either direct or indirect (vicarious) liability. The former refers to the liability that is attached to the organisation or a company when they themselves direct or authorise the employee to act in a certain way. In *Tesco Supermarkets Limited v Nattrass* [1972] AC 153 Lord Reid held that this direct liability occurs when a person is *not acting as a servant, representative, agent or delegate* of the company but as *an embodiment of the company.*

On the other side of the fence, vicarious liability may be attached to employers for the acts of their employees in the course of their employment. The key question for such liability is whether the employee was acting *in the course of his employment* at the time in question. In *Jones v Tower Boot Co Ltd.* [1997] IRLR 168 the Court of Appeal held that this phrase should be given its ordinary meaning and should not be construed restrictively. Latham CJ applied a broad interpretation of the concept in *Deatons Property Ltd v Flew* [1949] 79 CLR 370 where His Lordship held that an act is within the scope of his employment if the employee was retained to perform the act, or if its performance is reasonably incidental to the matters which the employee was retained to do.

WORKPLACE SEARCH

The US Supreme Court has held that whether an employee has a reasonable expectation of privacy in a workspace is to be decided on a case-by-case basis because of the great variety of workplace settings as was held in the case of *O'Connor v. Ortega* 480 U.S. 709. The Court also held that a public employer's intrusions, even into constitutionally protected privacy interests of government employees for either non-investigatory, work-related purposes

or for investigations of work-related misconduct, should be judged under a standard of reasonableness. The Court noted that the requirement for an employer to obtain a warrant whenever he or she wished to enter an employee's workspace for work-related purpose would seriously disrupt business routine and be unduly burdensome. In terms of workplace computer search, in the case *Leventhal v. Knapek* 266 F.3d 64, the Federal Court has held that an employee has a reasonable expectation of privacy in the contents of an office computer, but an investigatory search for evidence of work-related employee misconduct is constitutionally reasonable if the search is justified at its inception and is of appropriate scope (i.e., reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct).

In the private sector, employees may have a reasonable expectation of privacy in certain areas and personal items. In *K-Mart Corp. v. Trotti* 677 S.W.2d 632, the court has held that an employee who is under no suspicion of wrongdoing and secures a locker with her own lock and with the employer's consent has a reasonable expectation of privacy in the locker and its contents. In addition, employers may be liable if they reveal confidential information about their employees as decided in *Miller v. Motorola, Inc.* 560 N.E.2d 900 (Ill. App. 1990).

WORKPLACE SURVEILLANCE

Video surveillance to monitor the activities of employees is rampantly used by employers. An employer's use of video surveillance is permissible in US, where US courts have examined an employee's expectation of privacy in the area being monitored, as well as considered any applicable laws or regulations governing such a search. Federal courts have held almost unanimously that silent video surveillance is not prohibited by Title I of the Electronic Communications Privacy Act (ECPA) of 1986. But video surveillance that includes the ability to record conversations would violate Title I. This was decided in the case of *Thompson v. Johnson County Community College*, 930 F. Supp. 501 (D. Kan. 1996).

Video surveillance is used extensively for many different reasons. Australia spent substantially more money per capita than any other industrialised nation on video surveillance equipment. Video cameras are now one of the most commonly used surveillance devices in the Australian workplace, and their use is regulated by The Workplace Video Surveillance Act of 1998. Video surveillance is justified as a security measure to deter theft, vandalism, or other unauthorised intrusions, and to monitor employee conformance with occupational health and safety procedures, as well as general performance.

The use of video cameras and closed circuit televisions (CCTV) is another common way of monitoring employees within the workplace. Even areas where

employees would previously have enjoyed high expectations of privacy, such as bathrooms or locker rooms, have come under increasing surveillance. Postal workers in New York City found hidden cameras in restroom stalls and waiters in the Boston Sheraton were secretly videotaped in the hotel locker room. Where staffs are more mobile, companies are now using a range of technologies to track geographic movements (Hartmann, 1999). Some hospitals now require nurses to wear badges on their uniforms so they can be located constantly (Auchard, 2001).

TELEPHONE MONITORING

Employers have broad discretion to monitor employees' calls for *business purposes*. A British program called *Watcall*, produced by a company called Harlequin, can analyse telephone calls and group them into *friendship networks* to determine patterns of use. Voice mail systems are also subject to systematic or random monitoring by managers (Davies, 1997). In US, Title III of the ECPA has numerous exceptions. In the workplace, two exceptions are most often cited. The first exception is *consent* by one-party, as the ECPA provides that *a party to the communication* may intercept and may give *prior consent* to intercept, even when the other party is unaware of the interception. This one-party consent need not be express and may be implied from *surrounding circumstances*, including knowledge of the interception. The second exception, which is often termed the *ordinary course of business* exception, allows the use of: any telephone or telegraph instrument, equipment, or facility, or any component thereof, (i) furnished to the user by a provider of wire or electronic communication service in the ordinary course of its business or (ii) being used by a provider of wire or electronic service in the ordinary course of its business.

Referring to the case of *Watkins v. L. M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983), where the defendant Berry Co. employed plaintiff Carmie Watkins to sell advertising by telephone from Berry Co.'s office. Berry Co. had "an established policy, of which all employees are informed, of monitoring all solicitation calls as part of its regular training program." Employees were permitted to make personal calls, but were not told whether those calls would be monitored. A friend telephoned Ms. Watkins at work about a new job, and Berry Co. monitored the call. Ms. Watkins sued. The District Court granted summary judgment for Berry & Co., finding both implied consent and a business interest in the monitoring. The Court of Appeals reversed. "Consent is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasion on which interception may lawfully take place ... Knowledge of the capability of monitoring alone cannot be considered implied consent", the learned trial judge said. As for the ordinary course of business exception, the Court stated:

> It is not enough for Berry Co. to claim that its general policy is justifiable as part of the ordinary course of business. We have no doubt that it is. The question before us, rather, is whether the interception of this call was in the ordinary course of business. In the ordinary course of business" cannot be expanded to mean anything that interests a company. We hold that a personal call may not be intercepted in the ordinary course of business ... except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents. (p. 582, 583).

In *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992) plaintiff Sibbie Deal was employed in a store owned by defendants Newell and Juanita Spears. The defendants asked Ms. Deal "to cut down on her use of the store phone for personal calls, and the Spearses told her they might resort to monitoring calls" Later, the store was burglarised. "The Spearses believed it was an inside job and suspected ... Deal". " The Spearses then installed a tape recorder for calls in the store, with no indication to the parties using the phone that their conversation was being recorded. Over seven weeks, the Spearses taped 22 hours of Ms. Deal's calls, including sexually provocative conversations with a non-employee. Ms. Deal sued. The Spearses' defences included consent and ordinary course of business. At trial, the District Court rejected the defences and awarded $40,000 in statutory damages plus attorneys' fees. The Eighth Circuit affirmed. On consent, the Court stated that:

> The Spearses did not inform Deal that they were monitoring the phone, but only told her they might do so in order to cut down on personal calls. Moreover, ... the couple anticipated Deal would not suspect that they were intercepting her calls, since they hoped to catch her making an admission about the burglary ... (p. 1157).

And as for ordinary course of business, the Court said that:

> The Spearses had a legitimate business reason for listening in: they suspected Deal's involvement in a burglary ... and hoped she would incriminate herself. Moreover, Deal was abusing her privileges by using the phone for numerous personal calls ... when there were customers in the store. The Spearses might legitimately have monitored Deal's calls to the extent necessary to determine that the calls were personal and made or received in violation of store policy. But, the Spearses recorded twenty-two hours of calls,

and ... listened to all of them..., Deal might have mentioned the burglary at any time during the conversations, but we do not believe that the Spearses' suspicions justified the extent of the intrusion. The scope of the interception in this case takes us well beyond the boundaries of the ordinary course of business (p. 1158).

Based on the above cases, a few principles have been established by the Courts in US. Firstly, employer ownership of the communications equipment alone is not carte blanche to intercept employees' communications. Secondly, the ordinary course of business exception often requires an employer (as the equipment's owner) to prove: (a) it had a particular reason for intercepting particular communications, and (b) it took reasonable steps to intercept nothing more. In other words, this exception does not always allow blanket interception, especially of employees personal communications. Thirdly, implied consent must be based upon employees' clear and prior knowledge that their communications will be intercepted. Knowledge that communications can be or might be intercepted is likely insufficient.

E-MAIL AND INTERNET USE MONITORING

Computers and networks are particularly conducive to surveillance. The Privacy Foundation study in 2001 (Schulman, 2001) showed that 14 million employees in the US are subject to this kind of surveillance on a continuous basis. Employers can monitor e-mail messages by randomly reviewing e-mail transmissions, by specifically reviewing transmissions of certain employees, or by selecting key terms to flag e-mail. Some programs used by employers can even use algorithms to analyse communication patterns and turn them into images. Monitors can then look at these images to follow traffic patterns and detect whether sensitive data is at risk.

Many employers rely on software for remote monitoring of e-mail messages. With a few clicks they can see every e-mail message that employees send or receive and determine whether they are *legitimate* or not. Employers give a variety of reasons for installing such software. Some say it is to protect trade secrets or preventing sexual harassment incidents. Others want to prevent oversised-mails clogging networks and using too much bandwidth. Still others simply that they do not want employees wasting company time by using these systems for personal activities.

According to the American Management Association (2001), nearly two thirds of all companies discipline employees for abuse of e-mail or Internet connections and 27% had dismissed employees for those reasons. In 2000, Dow Chemical Company fired 50 US employees and threatened 200 others with suspension after they found offensive material in their e-mail. The company

opened the personal e-mail of more than 7,000 employees. Similarly, the New York Times fired 23 employees in 1999 for sending obscene messages.

In 2000, Hong Kong the Office of the Privacy Commissioner for Personal Data (2000) commissioned a survey to examine employer surveillance in the workplace. According to the survey, 64% of employers had installed at least one type of employee monitoring equipment, but only 18% of the employers had a written policy on employee monitoring. Furthermore, 35% of respondents did not even know whether such a policy existed.

In contrast, France has established stringent policies that protect the privacy of employees' e-mail usage. The French Supreme Court held recently in the case of *Nikon v. Onof*, Decision No. 4164, October 2, 2001 (99-42.942) that employers do not have the right to open any of their employees' messages. The Court ruled in a case between Nikon and a former employee that the company had no automatic right to search through an e-mail inbox.

Courts in the US have taken various positions in cases involving an employee's use of e-mail and the Internet at work. In *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), the Court found that an at-will employee has no reasonable expectation of privacy in the contents of an e-mail voluntarily sent on an employer's e-mail system, even though the employer had assured its employee's that e-mail communications would remain confidential and privileged. The court reasoned that once an employee communicated comments to a second person over an e-mail system utilised by the entire company, any reasonable expectation of privacy is lost. And even if an employee had a reasonable expectation of privacy in the contents of an e-mail, a reasonable person would not consider an employer's interception of such communications to be substantial or highly offensive. In another case of *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) it was held that an employer that has a business use only policy for Internet usage may conduct audits of its computer network to identify, terminate, and prosecute unauthorised activity. The court found that while employees may have a legitimate expectation of privacy in their computer equipment, some office practices, regulations, or procedures may reduce such an expectation.

Title III of ECPA on definition of electronic communication includes e-mail and Internet use. However, the Title III definition contains a major hole: electronic communications not include such communications in electronic storage. In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), plaintiff Steve Jackson Games, Inc. (SJGI) had an electronic bulletin board which offered customers the ability to send and receive private E-mail. Private E-mail was stored ... temporarily until the addressees 'called' ... (using their computers and modems) and read their mail". Defendant United States Secret Service read "162 items of unread, private E-mail". SJGI sued. The District Court entered judgment for the Secret Service on SJGI's

Title III claims, because the e-mail was not acquired by the Secret Service "contemporaneous with the transmission of these communications". The Fifth Circuit Court of Appeals affirmed and observed that unlike the definition of 'wire communication' the definition of 'electronic communication' does not include electronic storage of such communications".

Likewise, in *Bohach v. City of Reno*, 932 F.Supp. 1232, 1236 (D. Nev. 1996) the city's police department had an *Alphapage* system. A police officer could communicate with another officer by typing on a keyboard connected to a computer. The police chief had warned all users that every message is logged on the network. However, the chief had not warned officers that messages were automatically stored, and it was unclear what officers understood. The city retrieved old, stored messages for use in an internal affairs proceeding. Citing Title III, two officers moved to enjoin such use. The District Court denied the motion:

> All messages are recorded and stored not because anyone is tapping the system, but simply because that's how the system works. It is an integral part of the technology ... E-mail messages are, by definition, stored in a routing computer. An electronic communication may be put into electronic storage, but the storage is not itself part of the communication. The statutes therefore distinguish the "interception" of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into "electronic storage" (p. 1234-1236).

In *Garrity v. John Hancock Mutual Life Insurance Co.*, 18 IER Cases 981 (Mass. Dist. Ct. 2002), two insurance company employees obtained and distributed sexually explicit e-mails through the company's electronic system. A co-worker complained to management of receiving such emails, prompting an immediate investigation, which resulted in checking the employees' e-mail folders as well as the folders of fellow co-workers to whom they had previously sent e-mails. The two implicated employees claimed that their personal e-mail was private since the company had encouraged them to have personal passwords and set up personal email folders. Despite these contentions, the federal district court found that this expectation of privacy was unreasonable for several reasons. One of the most important reasons behind the court's decision was the company's detailed, published e-mail policy in which employees were told that certain e-mails were not allowed on the company system and that violation of this policy could result in disciplinary action up to and including termination of employment. The court also relied on a series of cases from other jurisdictions, which stated that even in the absence of such a company policy, the voluntary submission of personal comments over a system used by the entire company negates any privacy interests in such communications. Additionally, the court

rejected any notion that by creating a personal password or folder, employers forfeit the right of inspection of email files used by employees but maintained by the company. Lastly the court held that even if a reasonable expectation of privacy could be found, the employer's legitimate business interest in protecting employees from harassment trumps these privacy interests. Allowing employees to use a company e-mail system to distribute offensive or harassing materials to fellow co-workers, could subject employers to potential liability for harassment or other forms of discrimination. Thus, an employer's interest in preventing the dissemination of certain materials is clearly legitimate.

Garrity's case may serve as a guideline for employers and courts alike - particularly since more private sector employers are publishing company policies that limit employees' expectations of privacy, even where privacy might normally be presumed.

These abovementioned cases raise complex legal and ethical questions concerning an employee's fundamental right to privacy and due process, such as: what if an employee is sent an *offensive* e-mail, accidentally or maliciously? The e-mail cannot simply be deleted. It remains logged on the company server, threatening the relationship of trust between employee and management. Or what if an employee is dismissed on the grounds of sensitive personal information (for example issues relating to sexual preferences, medical conditions, etc.) gathered through a system? This problem also arises when companies monitor all Internet activity looking for visits to *inappropriate* sites. Such surveillance has elements in common with traditional surveillance for hard copy pornography, but there are significant dangers to workers in the realm of electronic surveillance. An employee may accidentally visit a pornographic site upon opening a spam e-mail that links to such a site. Or websites may be accidentally visited when displayed as a hit in response to a perfectly innocent search query. The surveillance technology does not, however, distinguish between an innocent mistake and an intentional visit.

The monitoring of chat room visits has also created some distress at the workplace. There is an increasing trend among companies to dismiss or sue employees for divulging company *trade secrets* or defaming the company in chat rooms. These have become known as *John Doe* cases. Because most people log on to chat rooms anonymously or use an alias, once a company observes a certain party in a chat room engaging in *illegitimate* speech, they must subpoena the message-board services such as Yahoo! or America Online, to obtain the identity of the specific author. The service providers often turn over identifying information when presented with a subpoena without any notice to the individual. The number of these cases is rapidly increasing and threatens not only the privacy of employees but also their rights to anonymity and free speech.

Employers and employees are concerned about computers in the workplace. Employers worry that employees waste time, such as, by chatting or shopping on-line. Employers worry too that employees create liability by viewing and circulating pornographic, racist, or other improper material.

WORKPLACE PRIVACY IN MALAYSIA: THE LAWS

As mentioned earlier, the Federal Constitution of Malaysia does not specifically recognise the right to privacy, but does provide for several related rights, including freedom of assembly, speech, and movement under Article 10 of the Federal Constitution. Other related statutes also limit the rights of individual privacy, for instance, section 39 of the Anti-Corruption Act 1997 empowers the Attorney General to authorise the interception of mail and the wiretapping of telephones in corruption investigations. Section 234 of Communications and Multimedia Act 1998 prohibits unlawful interception of communications, and under section 245 up to section 247, further establishes rules for search of computers, mandates access to encryption keys, and authorises police to intercept communications without a warrant if a public prosecutor believes a communication is likely to contain information relevant to an investigation. However, in practice, the provisions of the Communication and Multimedia Act 1998 restricting telecommunications interception appear to be regularly ignored or overridden by other statutes, including section 30 of Internal Security Act 1960 and section 10(2) and (3) Computer Crimes Act 1997. Last but not least, the newly introduced Anti Money Laundering Act 2000 as well empowers the intrusion of individual privacy especially relating to their bank account. These provisions show that rights to privacy are recognised but limited in its application.

WORKPLACE PRIVACY: THE MALAYSIAN POSITION

With regard to privacy of employee in workplace, there is no specific law that governs this issue. The former Deputy Prime Minister, Datuk Seri Abdullah Hj. Ahmad Badawi (2002) in a press conference stated that there is no specific law to allow the termination of ontract of service of any public servant who surfs obscene websites by using office computers during working hours. He added that only a disciplinary action can be taken against the public servant for misusing office facilities. However, Executive Director of Malaysian Employers Federation (MEF), Encik Shamsuddin Bardan insisted and suggested that employees who surf obscene websites during office hours should be terminated for misusing office facilities (Utusan Malaysia, 2002). As such, action can still be taken against any Malaysian employees who misuse any office facilities for personal use. In other words, the employees are subject to any surveillance and monitoring by their employer.

However, 38% of Malaysian employees believed that their data are safe and are not being misused by their employer. This was based on the survey by Asian Ideal MasterCard (2001). On the other hand, Malaysian employees are very cautious in using the telephone for personal use since they believed their conversations are open to interception by their employer (Utusan Malaysia, 2001).

MALAYSIA PERSONAL DATA PROTECTION BILL

The Ministry of Energy, Communications, and Multimedia has tabled a new piece of legislation on Personal Data Protection where the aim of the Bill is to regulate the collection, possession, processing, and use of personal data by any person/organisation so as to provide protection for an individual's personal data and safeguard the privacy of an individual, and to establish a set of common rules and guidelines on handling and treatment of personal data by any person/organisation.

Under this Bill, the term *personal data* is defined to mean any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual. (S 2 of the Bill) The bill further defines the term data subject and data user. *Data subject* means "an individual who is the subject of personal data" (S 2 of the Bill) and *data user* means "a person who either alone or jointly with other persons, controls the collection, holding, processing or use of the personal data but does not include any person who collects, holds, processes or uses solely on behalf of another person" (S 2 of the Bill). As such, those who collect materials for a third party will not fall under the definition.

Any type of processing of personal data will have to be in compliance with all the data principles. Here, the term process is defined widely to mean, "the carrying out of any operation or set of operation on any personal data and includes recording, amendment, deletion, organisation, adaptation, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction or dissemination of the personal data" (S 2 of the Bill). This means that where files are only retrieved, it is already considered as being processed, and therefore is subjected to those data principles. S 4 of the Bill requires that all data principles in the schedule is to be complied with whenever any personal data is collected, held, processed, or used by a data user. These principles are:

(1) Principle 1 - Manner of collection of personal data. Data must be collected fairly and lawfully. The data user must also be informed of when and

what personal data is collected and the purpose for which the personal data are to be used.

(2) Principle 2 - Purpose of collection of personal data. The purpose of collecting the data must be specified and lawful. In this regard, the collection of data is lawful if it relates directly to a function or activity of the data user, or necessary for that purpose. The data collected must also be adequate, relevant, and not excessive in relation to the purpose.

(3) Principle 3 - Use of personal data. Personal data collected must only be used for the purpose in which the data is collected or any other purposes directly related to that. Once the purpose of collecting the information ceases, the personal data must be erased, unless such erasure is prohibited under any law or against public interest.

(4) Principle 4 - Disclosure of data. Personal data must not to be disclosed unless in relation to the purpose in which it is collected. In relation to this, s 42 contains certain exceptions such as: (a) the data subject or relevant person has consented to the disclosure, (b) the disclosure is necessary for the purpose of preventing or detecting crime, (c) disclosure is required under the law, or (dis)closure is justified as being in the public interest.

The data subject may withdraw his consent for the disclosure of his personal data. In this instance, the data user has a duty to cease to hold, process, or use, the personal data.

CONCLUSION

In conclusion, most employers believe that since they have ownership or control over the working premises, and its contents and facilities, that employees give up all rights and expectations to privacy and freedom from invasion. Others simply avoid the question by making employees consent to surveillance, monitoring, and testing as a condition of employment. However, we have seen that various countries in the world recognise the privacy of the employees in their workplace, though, of course, this is not absolute. In the US, ECPA is one piece of a very important legislation that recognizes the right of privacy in general, though the courts have typically been slow to recognize employees' rights to privacy. In *Whalen v. Roe* 429 U.S. 589 (1977) a constitutional right to information privacy is recognised and it was held that it can protect against employer disclosures of employees' personal information.

In European countries (European Commission, 2002), the collection and processing of personal information is protected by the EU Data Protection and the Telecommunication Privacy Directives. For example, Austria, Germany, Norway, and Sweden have strong labour codes and privacy laws that directly or indirectly

prohibit or restrict this kind of surveillance. In Finland, a new law on Data Protection in Working Life entered into force in October 2001. In October 2000, the United Kingdom Privacy Commissioner issued The Employment Practices Data Protection Code, a draft code of guidance for employer/employee relationships. In 1999, the Swedish government established a Committee to study workplace privacy issues. In March 2002, the Committee issued a proposal recommending specific legislation to protect the personal information of current employees, former employees and employment applicants in both the private and public sectors.

In Asia, Hong Kong had formed in June 2002, the Hong Kong Data Protection Commission and issued a draft code of practice on workplace for public consultation (2002). The draft code covers telephone, closed-circuit television, e-mail and computer usage and possibly location monitoring. In Australia, the Privacy Amendment (Private Sector) Act 2000 put in place limit restrictions on employers monitoring of communications by requiring the establishment of formal e-mail use policies that must be made clear to all employees. It also requires employers to prove that the monitoring of e-mails is justifiable-for instance, on grounds of employees' excessive use of e-mail, distributing offensive material, suspected criminal activities, or passing on of sensitive information (Law Reform Commission New South Wales, 2001).

As such, it is a lauded move by the government of Malaysia to introduce Personal Data Protection Bill or any law which has the same effect of Personal Data Protection 1998 in UK or ECPA in US which clearly provide for the protection of individual privacy. It is submitted that the protection should be put into piece of legislation, not by just self regulation. To support, in *McVeigh v. Cohen*, 983 F. Supp. 215, 220 (D.D.C. 1998) the Court observed:

> ... in these days of 'big brother', where through technology and otherwise, the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.

REFERENCES

A Draft Code of Practice on Monitoring and Personal Data Privacy at Work, Office of the Privacy Commissioner for Personal Data. (2002, June 1). Retrieved March 14, 2007, from http://www.pco.org.hk/textonly/english/ordinance/files/ consult_ paper.doc.

ACLU, Workplace Rights, Electronic Monitoring. (n.d.). Retrieved June 22, 2005, from http://www.aclu.org/library/pbr2.html.

American Management Association. (2001). *Annual survey on workplace monitoring and surveillance 2001.* Washington DC, USA: Electronic Privacy Information Center.

Anti-Corruption Act 1997
Anti Money Laundering Act 2000
Communication and Multimedia Act 1998
Computer Crimes Act 1997
Data protection at work: Commission proposes new EU framework to European social partners (n.d.). Retrieved 11 April, 2007 at http://europa.eu.int/comm/employment_social/news/2002/nov/181_en.html.
Dow Chemical fires employees over inappropriate e-mails (July 27, 2000). Retrieved 22 June, 2005, fromt www.ABCNEWS.com.
Edward, B. (1964). Privacy as an aspect of human dignity, *New York University Law Review, 39, 971.*
Electronic Communications Privacy Act 1986
Eric, A. (2001, May 29). Monitoring shrinks worker privacy sphere. *Reuters.*
Federal Constitution (Malaysia)
Hartman, L.P. (1999, March 22). The economic and ethical implications of new technology on privacy in the workplace. *Business and Society Review.*
Helene, Z. (2001, June 26). Email snooping almost banned. *Information Technology News Service.* Retrieved 15 June 2005, from http://it.mycareer.com.au/news/2001/06/26/FFXDJRS4DOC.html.
Internal Security Act 1960.
Law Reform Commission New South Wales (2001). *Report 98, Surveillance: An interim report.* Retrieved 10 April, 2007, from http://www.lawlink.nsw.gov.au/lrc.nsf/pages/r98chp07.
Office of the Privacy Commissioner for Personal Data of Hong Kong. (2002). *Draft Code of Practice on Monitoring and Personal Data Privacy at Work.* Retrieved 10 April, 2007, from http://www.pco.org.hk/english/ordinance/codes.html.
Pekerja layari laman web lucah dikenakan tindakan disiplin. *Utusan Malaysia* (2002, July 13). Retrieved 10 April 2007, from http://www.utusan.com.my/utusan arc hive.asp?y=2002&dt=0714 & pub=utusan_malaysia&sec=muka%5Fhadapan&pg = mh _ 07.htm& arc=hive.
Personal Data Protection Bill
Ramai rasa selamat dengan rekod pekerja. *Utusan Malaysia* (Mac 10, 2001). Retrieved 11 April 2007, from http://www.utusan.com.my/utusan/archive.asp?y=2001&dt=0311&pub=utusan_malaysia&sec=ekonomi&pg=ek_06.htm&arc=hive.
Smith, R.E. (2000). Ben Franklin's Web Site 6 *Privacy Journal* (Sheridan Books 2000) online. Retrieved from http://www.privacyjournal.net/.
Schulman, A. (2001). The extent of systematic monitoring of employee e-mail and internet use. *Privacy Foundation.* Retrieved 11 April 2007, from http://www.sonic.net/~undoc/extent.htm.

Simon, D. (1997, April 29). Watch out for the Old Bill, *Daily Telegraph.*

Standler, R.B. (1997). *Privacy Law in the USA.* Retrieved 11 April 2007, from http://www.rbs2.com/privacy.htm.

Talib, N. (2003). *Law of torts in Malaysia.* Sweet & Maxwell Asia: Malaysia.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review,4,* 193-220.

Zaiton Hamin. (2001). E-mail @ work: Its legal implication on employer's liability. *Malayan Law Journal,3, xxviii.*