International Journal of Asian Social Science
ISSN(e): 2224-4441
ISSN(p): 2226-5139
DOI: 10.18488/journal.1.2018.87.332.345
Vol. 8, No. 7, 332-345

URL: www.aessweb.com

MODERN MEANS OF COLLECTING EVIDENCE IN CRIMINAL INVESTIGATIONS: IMPLICATIONS ON THE PRIVACY OF ACCUSED PERSONS IN MALAYSIA

Kamal Halili Hassan[1+]
Adam Abdelhameed[2]
Noorfajri Ismail[3]

[1,2,3]*Faculty of Law, Universiti Kebangsaan Malaysia*

(+ Corresponding author)

Article History
Received: 3 April 2018
Revised: 23 April 2018
Accepted: 25 April 2018
Published: 27 April 2018

Keywords
Modern means
Evidence collection
Criminal investigation
Accused privacy
Malaysia.

ABSTRACT

The article explores the implications of evidence collection in criminal investigations or proceedings on the privacy of accused persons in the Malaysian legal system. Modern evidence collection involves the use of technology and equipment to undertake electronic surveillance, wiretapping, and to access data stored in computers. Such methods have the potential to implicate the privacy of accused persons during criminal investigations or proceedings. This article first examines whether the Malaysian constitution and statutes provide for and protect the right to privacy. Assuming that they do, the question then is the extent to which the Malaysian Criminal Procedure Code (CPC) and Evidence Act (EA) extends to accused persons. As such, this article discusses the CPC and EA and other modern legislations such as the Digital Signature Act 1997, the Computer Crimes Act 1997, the Telemedicine Act 1997, the Communications and Multimedia Act 1998, the Electronic Commerce Act 2006, the Electronic Government Activities Act 2007, and the Personal Data Protection Act 2010.

Contribution/ Originality: This study contributes in the existing literature relating to cybercrime and at the same time, the study strengthened the nexus between cyber law and criminal justice to balance the interest between the public interest and individual privacy rights.

1. INTRODUCTION

The use of modern technology by law enforcement agencies in criminal investigations or proceedings has the potential to implicate the right to privacy of suspects or accused persons. The means employed such as electronic surveillance, wiretapping, and eavesdropping to collect evidence by enforcement agencies in criminal investigations have implications on the privacy rights of these persons. Beginning from the late 1960s the computer has been used as a medium for data storage (Adler, 1996). In later developments, computer networks came into existence (Adler, 1996) where a non-physical world has been created through the connecting of millions of computer users to thousands of electronic information storehouses worldwide (Kirby, 1996). This has raised questions with regard to privacy and turned the attention to the implications on privacy when computer data or information collected from

any of the activities on the internet is used as evidence in criminal proceedings. The absence of laws that adequately protect privacy against invaders using modern technology lead to unfortunate consequences including humiliation and social stigma and suicide of the ones whose privacy was invaded.

With the success of the technological advancement in the different fields of our lives, law enforcement agencies in criminal investigation or proceedings have resorted to technological devices in gathering evidence about a committed offence and the possible offender. Modern means of collecting evidence by enforcement agencies take in many forms. The enforcement agencies could use surveillance and tracking devices such as the global positioning devices (GPS), installing and listening devices to overhear suspects' conversation, seizing suspects' personal computer or other data storage devices, tracking suspect's emails accounts or online activities such as in social media or chat rooms, DNA analysis, thermal imaging, and aerial surveillance and imagery. All these technologies are used by law enforcement agencies either in conventional or cyber-crimes (Duryana, 2012). These have raised questions and controversies with regards to the implications of their use for law enforcement purposes on the suspect or accused's privacy right. The problem with these new technologies is that they are used in law enforcement purposes before the introduction of the legal framework that regulates their use.

The basis of discussion in this article will be the Malaysian legal system. Modern means of information and evidence collection will be discussed against the provisions in the legal system in order to explore whether or not they address the implications of the means used. This article is divided into two sections: the first explores the situation in civil claims while the second deals with the state of privacy rights in statutes.

1.1. Do Malaysian Courts Recognise Privacy Rights?

A pertinent question in regard to the legal status of privacy in Malaysia is whether Malaysian courts recognise such rights. We can look for the answer from judicial pronouncements in either criminal or civil case. The recognition of privacy rights on accused persons during criminal investigations or proceedings has so far not been dealt with by the Malaysian courts. Thus we have to draw an analogy on whether such rights exist in civil proceedings. There is a case in which a high court ruled in a matter involving electronic surveillance as one of the modern means based on the provisions of the constitution. In a civil proceeding, the Johor Bahru High Court ruled in favour of the plaintiffs' claims on privacy invasion in *Lew Phow @ Lew Cha Paw & 11 Ors v. Pua Yong Yong & Anor* [2009] 1 LNS 1256 that involved the use of CCTV cameras. The Court not only recognized the privacy rights per se in this case but also accepted claims on the invasion of privacy as a result of the use of modern means. The ruling is significant in being the first of its kind in the country to deal with this controversial matter.

As far as civil claims are concerned, there is also a case involving modern means in the form of photography that was heard by the High Court of Pulau Pinang. In the *Lee Ewe Poh v. Dr. Lim Teik Man & Anor* [2010] 1 LNS 1162 it was claimed that the private parts of the plaintiff were photographed by her surgeon, and this case is considered the first ruling in the country in which privacy invasion was recognized as an actionable tort (Foong, 2011). In this case, the plaintiff asked for an injunction prohibiting the defendant from dissemination of her photographs to other people. The court found that the said photographing represents an actionable invasion of privacy under civil claims.

Besides the above, other similar cases are currently awaiting judicial outcomes. Like people elsewhere, Malaysians are experiencing invasions of their privacy as a result of the use of modern technologies such as surveillance cameras and photography. It is not clear, however, whether cases such as that of the Member of Parliament, Datuk Rahman Ismail, who was taped in a hotel room with a female who was not his wife and that of intimate photos of Elizabeth Wong with her lover that were made public (Murni and Ratnawati, 2011) will be heard before the lower courts. Other cases include that of Dr. Chua Soi Lek who was videotaped having an extra-marital affair in a hotel and the footage uploaded onto the internet that led to his resignation as a minister, as well as the case of actress Nasha Aziz where cameras installed in her house videotaped her daily activities that included footage

of her being in a state of undress (Murni and Ratnawati, 2011). If the High Courts or the Federal Court have to rule on the above-mentioned cases, they will undoubtedly face difficulties in interpreting whether the provisions in the federal constitution provide for privacy protection or not. In addition, the lack of precedents for handling such civil and judicial claims will also be problematical.

However as indicated before, in the area of law enforcement in criminal investigations or proceedings, there is no reported case to show the direction of court decisions in understanding and applying the constitution. As indicated earlier, the constitutional provisions arguably apply only to the activities of the federal and state governments. This means that they protect privacy against infringements by law enforcement agencies in collecting evidence in criminal investigations or proceedings. Based on this, if the courts are presented with a case involving privacy invasion by law enforcement agencies, they should take into consideration the suggestion made in this respect. According to Foong Cheng Leong, precedent should be followed in strip searches and searches of premises and vehicles conducted by law enforcement agencies in establishing whether they constitute infringement of privacy and to exclude evidence obtained through any such infringement (Foong, 2011).

Compared with the US legal system, the constitution and civil claims in Malaysia provide little protection to privacy where modern technology is involved. As seen above only two cases were decided by courts in Malaysia. Invasions of privacy in the US using such means are mainly addressed with the reference to constitutional provisions. The position of the Malaysian legal system in this matter will be clearer when cases pending before the courts are finally heard.

1.2. Are There Privacy Rights in the Statutes?

In examining the statutes on privacy protection involving modern means of evidence gathering in criminal proceedings, the Criminal Procedure Code and the constitution will be referred to as the main laws in investigations that use both conventional and modern means (Duryana, 2012). The remaining statutes are the ones introduced in the country in response to technological advancements, i.e., cyber laws to address issues relating to the use of technology in modern life. As indicated earlier, Malaysia has reviewed its existing legislations as well as enacted new ones for this purpose. It has amended the Copyright Act, the Evidence Act, the Interpretation Act, and the Companies Act. New laws enacted are the Digital Signature Act 1997, the Computer Crimes Act 1997, the Telemedicine Act 1997, the Communications and Multimedia Act 1998, the Electronic Commerce Act 2006, the Electronic Government Activities Act 2007, and the Personal Data Protection Act 2010.

It goes without saying that each of the above laws governs a certain area of activity of the activities performed in cyberspace. However, this article is not meant to provide detailed areas of coverage of each law since some of their provisions are found in existing legislation such as the Penal Code. As such, only a brief discussion of the rationale behind the enactment and the scope of application will be provided as a background to protection of privacy rights issues in these laws. For the purposes of exploring whether existing statutes address the implications of modern means used by law enforcement officials in criminal investigations or proceedings, it is observed that while some of the legislations provide little, general, or no protection to privacy, only some of the legislations regulates privacy invasion in criminal investigations or proceedings. Following is a discussion of each of the two categories.

The statute that provides general protection is the Penal Code. As indicated earlier, the code provides protection to privacy under Sections 292, 293, 294 and 509. In the first three Sections, privacy is protected in the context of the protection against exposure to obscene materials such as books, songs, and other objects through the acts of selling, letting to hire, distributing, publicly exhibiting, etc. In Section 509, protection is afforded to privacy in connection to modesty and human dignity. As seen in *Kong Lai Soo v. Ho Kean* [1973] 2 MLJ 150 and *Maslinda Ishak v. Mohd Tahir Osman & Ors* [2009] 6 MLJ 826 the courts had at the outset to ascertain that invasion of privacy was committed through uttering a word, making a sound or gesture, or exhibiting an object with the

intention to offend the modesty of the plaintiff. In the *Maslinda* case, in addition to being within the view of everyone in the truck, the invasion of privacy also involved photography of private parts similar to the *Lee Ewe Poh v. Dr. Lim Teik Man & Anor* [2010] 1 LNS 1162. It should also be reiterated that Section 509 of the Penal Code does not provide protection to all aspects of privacy but only to personal bodily or physical privacy that guards the person against physical accessibility by others (Burgoon, 1982).

It should be stated that the protection of privacy in the Penal Code is a general protection in nature. It protects privacy in the above-mentioned situation to everyone. It is not meant to protect the privacy of accused persons in criminal proceedings. However, it may apply to the accused if his or her privacy is invaded with the intention of offending modesty. This applies to situations in conventional means as well as to modern means of evidence collection used by law enforcement officials in criminal proceedings.

Among the statutes that provide little or no protection to privacy is the Telemedicine Act 1997. This Act was passed by the Malaysian legislature as a regulatory framework for the practice of the profession in the Multimedia Super Corridor (MSC). It encompasses the electronic transfer of data, images, voice and video, via telephone lines or satellites (Ranjan, 1997). The Act clarifies the concept of telemedicine and specifies clearly those who can provide medical services and carry out telemedicine as well as prescribes the penalties for those who practice this profession in violation of the requirements (Sections 2 and 3).

With regard to the protection of privacy rights, the Act was criticized for delivering little protection to private information provided by patients in the process of utilizing this platform (Zaharom and Mustafa, 1998). It stated, in Sub-section 5 (2)(d), that "any image or information communicated or used during or resulting from telemedicine interaction which can be identified as being that of or about the patient will not be disseminated to any researcher or any other person without the consent of the patient".

The other legislation in this category is the Copyright (Amendment) Act 1997 which was introduced to regulate the use of computer-stored information and curbing the violation of this information. These include computer programs and databases considered to be the most vulnerable to violation (Jayaseelan, 1997). The Act was amended in line with the rules and regulations suggested by the World Intellectual Property Organization (WIPO) Treaty or the WCT 1996. Through this Act, Malaysia has sought to address the challenges arising from the latest developments in technology and to provide further protection to multimedia contents through specifying the applicability of existing copyright and patent laws against computer software piracy (Ida Madieha, 2000). The amendment to the Act also aims at enabling Malaysia to realize the full potential of its MSC as it provides adequate legal protection to educational, entertainment and information contents in the MSC (Sangal, 1997).

The Act introduced three new offences under section 41 of the old Act and made them punishable with heavy penalties. These include circumventing or causing the circumvention of any effective technological measures, the removal or alteration of any electronic rights management information without authority, and the distributing, importing for distribution or communicating to the public, without authority, works or copies of works in respect of which electronic rights management information has been removed or altered without authority. With regard to privacy, the Act provides no provision that recognizes and protects this right.

As for the Evidence Act, it has been amended twice, in 1997 and in 2012, in recognition of the fact that the evidence system is not separable from other legislative efforts in the country. Under the Evidence (Amendment) Act 1997, the revision was made with the objective of introducing a new provision that regulate and govern admissibility of documents produced through electronic means in any proceedings in civil or criminal courts (Section 90A). For the Evidence (Amendment) (No. 2) Act 2012, Section 3 was revised to redefine the term "computer" to mean "an electronic, magnetic, optical, electrochemical, or other data processing device …". In addition, Section 114A was added on the "presumption of fact in publication" on the internet. The presumption allows for the prosecution or plaintiff to prove the identity of the person suspected of internet publication to be the publisher of the contents in question, i.e., the wrongdoer, unless proven otherwise. In other words, the section eases

proving of the offences enumerated in the cyber laws or other related laws. The presumption has been criticized for establishing the "presumption of guilt" and reversing the "presumption of innocence" that assumes the suspect to be innocent until proven guilty beyond reasonable doubt (Foong, 2012). Interestingly, the amendment is defended on the need to protect the public interest.

The amendments to the Evidence Act provide no new rules relating to criminal procedures including the search of persons and of premises. They were left to the general rules that exist in the Criminal Procedure Code. Thus no direct or indirect interest in privacy is shown in the provisions of this Act.

With regard to the Interpretation (Amendment) Act 1997, it provides effect to the use of electronic means related to information required under any statute in Malaysia to be given or maintained, provided that the identity of the person giving the information could be determined and verified and a sufficient precaution could be made to avoid unauthorized access to the information (Siddiqi, 1999). It could also be said that the Act, by its nature, makes no reference to privacy.

The Companies (Amendment) Act 1998, which entered into force in September 1998, gives recognition to electronic filing and documentation in e-commerce. It was introduced in support of the Digital Signature Act and the Computer Crimes Act which would be partially ineffective without this recognition (Siddiqi, 1999). Likewise, the Companies (Amendment) Act introduced no novel provisions with regard to the protection of the right to privacy, directly or indirectly. It left the matter to the general rules in the related legislations.

The other cyber legislation is the Electronic Commerce Act (ECA) 2006 which entered into effect on 19 October 2006. According to its preamble, the ECA was introduced to give legal recognition of the electronic messages in electronic commerce transactions, the use of electronic messages to fulfil legal requirements, and to enable and facilitate commercial transactions through the use of electronic means and other matters.

The ECA has been criticized for limiting the communication to commercial transactions (Section 2) rather than including other related matters such as statements, declarations, offers, demand, notice, and acceptance of an offer (Abu and Siti, 2009). It is also criticized for including additional requirements not found in international instruments and comparable legislations such as *intelligible* in Section 8 and for requiring the message to be accessible (Abu and Siti, 2009). On the right to privacy, although the Act regulates the message as a communication means, which is considered an important aspects of privacy, it has no provision protecting the right to privacy in electronic commerce transaction messages where users of this platform for shopping provide information about themselves.

Another effort in the area of cyber laws in Malaysia is the Electronic Government Activities Act (EGAA) 2007. According to its preamble, the Act aims at providing legal recognition of the electronic messages exchanged between the government and the public as well as the use of electronic messages to fulfil legal requirements and to enable and facilitate dealings through the use of electronic means and other related matters.

In making a comparison between the issues covered by the ECA and those of the EGAA, Chen Prins opines that several issues in the latter resemble those in the ECA such that the matter justifies being dealt with using a single comprehensive approach (Prins, 2007). This view is shared by Abu Bakar Munir and Siti Hajar Mohd. Yasin who feel that the EGAA is "redundant" and needless. They argue that the principles included in this Act are similar to those governing non-commercial activities under the ECA 2006 and that the regulations in the EGAA could have been achieved through an amendment of the ECA rather than enacting a separate new piece of legislation (Abu and Siti, 2009). Chen Prins, however, is of the opinion that the challenges involving government activities differ from those in electronic commerce activities due, among other things, to the fact that an electronic government is designed for "one-shop" multiple use as compared to electronic commerce in which each entity or platform designs its own requirements, as shown in the experience of many countries (Prins, 2007).

When it comes to the main focus of our article, privacy is said to be one of the most persistent legal issues that arise in relation to electronic government (Prins, 2007). Nevertheless, the EGAA provides no specific provisions in

this respect. It is argued that the Act includes no such provisions due to the legislature's inclusion of the protection of government activities in the Personal Data Protection Act 2010 and as such deems it needless to repeat the provisions (Zulhuda, 2012).

Compared with the situation in the US legal system, Malaysian statutes provide general, little, or no protection of privacy while the US sectoral statutes provide privacy protection to certain sectors or activities or category of persons. The laws that provide little or no protection are similar to their US counterparts which provide no privacy protection in the context of criminal proceedings. These include the statutes relating to credit reporting, financial modernization, identity theft, cable communication, videotape, telephone consumer, health insurance and education, among others.

2. STATUTES ON LAW ENFORCEMENT FOR CRIMINAL INVESTIGATION: HOW DO THEY AFFECT THE PRIVACY OF THE ACCUSED?

Heading the legislations related to law enforcement in criminal investigations and proceedings is the Criminal Procedure Code (CPC). Besides the CPC, some of the cyber laws created in Malaysia deal with privacy in relation to criminal procedures. In addition to its primary role in regulating procedures in conventional means of evidence collection, the CPC is a general reference for investigation of technology-related offences including cybercrime. According to Duryana Mohamed, in executing any search and seizure under cyber laws such as the Computer Crimes Act, investigating officers rely on the general rules set out in the CPC as a comprehensive law (Duryana, 2012). This means that although cyber laws regulate search and seizure, reference is made to the CPC during investigations conducted by law enforcement officers, including police officers or officers authorized by the Commission such as in the Communications and Multimedia Act.

In regard to the modern means of evidence collection, Subsections 116B and 116C were introduced in the 2012 amendment to the CPC to deal with searches and seizures involving computers and other storage devices and information contained in communications. Subsection 116B regulates access by law enforcement officers to data stored in a computer or other storage medium. It allows a police officer not below the rank of Inspector conducting a search to access data in storage media. It clearly provides for the admissibility of evidence obtained from such access in criminal proceedings. Subsection 116C provides the Public Prosecutor the power, if he considers that it is likely to contain any information related to the commission of an offence, to authorize a police officer to intercept any message transmitted or received by any communication as well as to intercept, listen to, and record any conversation by communications for law enforcement purposes. In addition, the Public Prosecutor also has the power, if he considers that it is likely to contain any information related to the commission of an offence, to require the communication service provider to intercept and retain specified communication or communications of a specified description received or transmitted or about to be received or transmitted by that communication provider. He is also provided with the same power to authorize a police officer to enter premises and install devices for the interception and retention of the said communication. It also accepts the admissibility of the information resulting from the said activities.

It should be noted that Subsection 116B gives the police officer the authority to access data in storage media without requiring the issuance of any warrant or order from a judicial body. This might jeopardize the privacy of the persons whose data is stored in the computer or storage medium subject to the search.

In addition, Subsection 116C allows the authorization given to service providers or police officers by the Public Prosecutor in the interception of communications and retention of the information intercepted as well as other related activities orally or in writing. It does not specify whether the oral or written authorization should be in the form of a warrant or an order. Warrants and orders differ with regard to the guarantees provided to privacy of persons related to the place to be searched and the things to be seized. Oral authorization also allows later correction of the situation.

Again, what is said about criminal procedure statutes in Malaysia and US in the conventional means can be said here. Firstly, criminal procedure codes in the two countries are the main sources of reference in the investigation for all the crimes including those related to technology. They provide similar provisions with regard to modern means used in law enforcement including communication interception, listening to or recording any conversation or communication, and entering premises for the installation of devices for the purposes of law enforcement as well as access to information in computers and other storage media.

There is also no difference between Malaysia's CPC and the US Rules of Criminal Procedure with regard to scientific evidence such as that provided by analysis of DNA samples. This is seen in the *Public Prosecutor v. Muhammad Rasid Hashim* [2011] 3 CLJ 424 involving a rape and murder in which the court relied on DNA found on murder weapons and on the deceased. It should be mentioned that there is also no reported case yet showing the use of some other modern means such as thermal imaging and aerial imagery and surveillance by law enforcement agencies.

The other legislation that deals with privacy in criminal proceedings is the Computer Crimes Act 1997 which was introduced to protect against computer exploitation and enacted to meet the provisions of the WIPO Copyright Treaty (WCT). It was based on the UK's Computer Misuse Act 1990 (Beatty, 1998) and Singapore's Computer Misuse Act 1993 (Siddiqi, 1999). It protects computers against misuse through stealing or destroying information stored in computers connected to the internet. It spells the acts and/or omissions that represent commission of the offences described therein and the penalties for each committed offence.

To strengthen the effectiveness of its provisions, the Act made abetments and attempts of offences punishable as offences (Section 7). It also provided rules contrary to the general principles in criminal law. Of these is the statutory presumption provided by the Act that any person who has in his custody or control a program, data, or other information which is held in any computer or retrieved from any computer without authority is deemed to have obtained unauthorized access to send program, data, or information unless the contrary is proved (Section 8). Nazura Abdul Manap and Hossein Taji criticized this presumption for establishing strict criminal liability as well as criminalizing the majority of computers users in the country as well as strengthening opportunities for gross abuse of police powers (Nazura and Hossein, 2012).

The presumption is also criticized by Beatty for removing the onus of proving (Beatty, 1998). In addition, Section 9 of the Act has also been criticized for extending its jurisdiction to offences committed outside Malaysia's national borders (Nazura and Hossein, 2012). According to Susan W. Brenner and Bert-Jaap Koops, this gives the Act "the widest possible jurisdiction scope, to the effect of establishing universal jurisdiction" (Brenner and Koops, 2004). In practice, prosecuting someone for cyber offences is problematic as an act that constitutes an offence in one country may be lawful in other countries (Brenner and Koops, 2004).

As far as privacy is concerned, the Act does not make explicit mention of this right. The statute is criticized by Murni Wan Mohd Nor and Ratnawati Mohd Asraf for providing little privacy protection. They recommend enhancing privacy protection through, among other means, incorporating this right explicitly in the constitution, enacting privacy legislation, or introducing stiffer criminal punishments, in order to ensure adherence to the rules stipulated in the law (Murni and Ratnawati, 2011).

However, it could be said that the Act contains provisions on the power to search, seizure, arrest, and obstruction of search in Sections 10 and 11 with the purpose of collecting digital evidence. Digital evidence is defined as evidence that involves computers or any other device that is capable of recording, storing, processing, retrieving or producing information (Duryana and Zulfakar, 2013). The CCA is one of the cyber laws that address the matter of privacy in relation to evidence collection as it regulates the search and seizure of computer data through which the electronic evidence is collected. Criminal procedures are clearly provided in the Act including search and seizure as well as arrest. Section 10 (1) provides police officers of or above the rank of Inspector the authority "to enter the premises, by force if necessary, and there to search for, seize and detain any such evidence".

It also entitles them to "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". Section 10 (2) allows the said police officer to enter the premises and conduct the search as detailed in Section 10 (1) even without a warrant provided that the officer has "reasonable grounds for believing that by reason of the delay in obtaining a search warrant the object of the search is likely to be frustrated". Searches of the premises is given to the specified police officers when they have reasonable cause to believe that there is concealed or deposited evidence of the commission of one of the offences enumerated in this Act (Wong, 2002).

In addition, Section 11 makes it a punishable offence for obstructing the police officers in entering and searching the premises as mentioned above as well as failing "to comply with any lawful demands of a police officer acting in the execution of his duty under this Act". The same criticism can be said about this legislation in terms of limiting its protection to some aspects of privacy.

Fortunately, Malaysian courts have been availed of the opportunity to rule in cases involving digital evidence related to computers. In the *Public Prosecutor v. Ong Cheng Heong* [1998] 6 MLJ 678, the court rejected the evidence by a witness who claimed no responsibility for a computer printout produced by him. Computer digital evidence is admitted by courts in Malaysia in three different forms, that is, computer evidence, computer output, and computer printout. In *Ahmad Najib Aris v. Public Prosecutor* [2007] 2 MLJ 505 the court was faced with the admissibility of computer evidence not produced in the course of the ordinary use of the computer. The document used as evidence was rejected by the court for not meeting the standards set out under Section 90(A)(6) of the Evidence Act 1950.

From the above cases it can be concluded that computer evidence is admissible as primary evidence in criminal proceedings in Malaysia as long as it is relevant, reliable, and authentic. Like any other evidence, certain measures should be adopted to protect evidence from being destroyed or altered in order to maintain its relevance, authenticity, and reliability (Duryana and Zulfakar, 2013). It should be mentioned that no comparable legislation is found in the US legal system.

Other legislation that meets the criterion of addressing privacy concerns in evidence collection by law enforcement officers in criminal proceedings is the Communications and Multimedia Act (CMA) 1998. Section 234 makes the interception, attempt to intercept, and procuring any other person to intercept or attempt to intercept any communication an offence punishable under the CMA. Sub-section 1 states that "A person who, without lawful authority under this Act or any other written law, intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any communications … commits an offence". Sub-section 3 states that "A person who commits an offence under subsection (1) … shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both".

The ultimate objective of the provision is to protect the confidentiality of information. Communication under this Section includes all means of communication such as electronic commerce transactions, e-mails instant messaging, social networking, sharing of files, web browsing, blogs, and chatting rooms (Siddiqi, 1999). This has led Maria Helena Barrera and Jason Montague Okai to call for a new paradigm in protecting online communication privacy due to the unique nature of digital correspondence compared to conventional physical means of correspondence (Barrera and Okai, 1999).

In addition, the Act provides indirect protection to some aspects of the right to privacy, personal privacy, and home privacy through sections that deal with criminal procedures including the power to investigate, search by warrant, search and seizure without warrant, and access to computerized data (Sections 246 through 252). These provisions are in line with the general rules in the CPC in regard to the abovementioned matters and seek to indirectly protect the right to privacy as stated earlier. However, it allows law enforcement officers to intercept communications, which is an infringement on the right of privacy.

Like the Computer Crimes Act, the CMA has been criticized for not providing adequate protection to privacy in general (Murni and Ratnawati, 2011). Nevertheless, it should be noted again that it provides regulations for

searches and seizures related to the internet executed by law enforcement officers (Section 246). Such law enforcement officers include police officers and public servants including magistrates or other persons needed for services rendered in connection with the detection of offence under the statute or its subsidiary legislation, or in relation to any forfeiture proceeding, or for any seizure made under this Act (Section 262) (Duryana, 2012).

It should be noted that the CMA includes privacy safeguards in criminal proceedings such as requiring search and seizure warrants. Section 247 provides details of the need for the warrants to meet the statute's requirement for search and seizure of places, persons, and things. These include reasonable cause to believe that an offence is being or has been committed or that any evidence or thing is necessary to the conduct of an investigation into an offence. It also provides special provision to protect the privacy of women by requiring them to be searched with women. Here, the CMA connects women's search with the same decency test found in the Penal Code. The Act is also in line with the Penal Code with regard to the exemption for conducting unwarranted search if there is a reasonable cause to believe that by reason of delay in obtaining a search warrant under that Section the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed (Section 248).

Interestingly, the CMA allows law enforcement officers to intercept or listen to any communication transmitted or received by any communication device if it is likely to contain any information which is relevant for the purpose of any investigation into an offence (Section 252). It permits this procedure with only an oral or written application of an authorized officer or a police officer of or above the rank of superintendent. However, the law prohibits the disclosure of the information intercepted or listened to from the communication (sub-section 5).

In relation to the implications of modern means, the issue of wiretapping was heard by the High Court of Melaka in *Telekom Malaysia Bhd v. Tribunal Tuntutan Pengguna & Anor* [2007] 1 MLJ 626. In this case, an unidentified person used the telephone line of the second respondent in making international calls while he was surfing the internet using a line connected to his telephone. The second respondent disputed the bill he was charged by *Telekom Malaysia Bhd*, the service provider, and filed a claim against the first respondent with the Consumer Claims Tribunal claiming that he had not made the international calls, but had only used the internet service, and that an international call was generated by the internet service without his consent. The Tribunal found in favour of the second respondent on the grounds that the computer of the second respondent was hacked and a wiretapping of the telephone line took place while the second respondent was surfing the internet.

The first respondent applied for a judicial review of the tribunal's award on the grounds that the award was beyond the tribunal's jurisdiction and therefore ultra vires. It submitted that the communications service involves electromagnetic waves and thus comes within the provisions of the Communications and Multimedia Act (CMA) 1998 and not the Consumer Protection Act 1999 unless otherwise prescribed by the minister, meaning jurisdictional error. The court ruled in favour of the first respondent. In addition, it stated that the issue raised is of immense importance and has far-reaching implications as it concerns public interest and affects every spectrum of telecommunication consumers nationwide and that the tribunal was established for the purpose of hearing claims for any loss suffered on any matter concerning consumer's interest. It concluded that the second respondent had elected the wrong forum for the dispute as it is outside the jurisdiction of the tribunal. It further gave the second respondent the choice to sue in a civil court of law or alternatively lodge a complaint on the basis of the provisions of the CMA for a resolution of the dispute and to get redress if any.

In this case, the relationship between wiretapping and the CMA was illustrated. It is hoped that this case will be treated as a precedent in future cases involving the use of wiretapping by law enforcement agencies for the purposes of evidence collection in criminal proceedings. The CMA is comparable to the US Electronic Communications Privacy Act (ECPA) 1986 as both regulate wire, oral, and electronic communications while in transit, and communication held in electronic storage. The US statute requires a warrant as well as an administrative request for conducting activities related to law enforcement. In addition, it allows many exemptions

that permit the interception of communications by law enforcement officers. The CMA allows such activities with only an oral or written application by an authorized officer or a police officer of or above the rank of superintendent but prohibits the disclosure of information intercepted or listened to from the communication.

The Digital Signature Act (DSA) 1997 which came into force on 1 October 1998 is another legislation related to privacy in law enforcement. It was enacted in order to encourage the adoption and use of electronic commerce. It tackles security and legal issues related to business transactions carried out through cyberspace and gives legal recognition to digital signatures (Jayaseelan, 1997). It also provides a degree of comfort to those using e-commerce. In recognition of the relative novelty of e-commerce, its Section 2 provides definitions of terms included in the Act. It also spells out several acts and/or omissions that are considered as offences as well as penalties to be imposed (Section 83). In making a comparison between the DSA and Singapore's Electronic Transaction Act (ETA) 1998, Zinatul A. Zainol concludes that the former focuses more on the legal recognition of digital signatures while the latter concentrates on giving the electronic commerce transactions the deserved legal recognition (Zinatul, 2000). With regard to protection of privacy, the DSA makes no direct reference to this right. Thus, it is also criticized for failing to protect consumer privacy (Lim, 1997). Protection of consumer privacy is important in Malaysia as consumers in the country are described to be "careless" about their personal data (Liau, 2013).

However, it can be said that the DSA indirectly protects privacy in criminal proceedings as it regulates them in relation to digital signatures in Sections 76 through 82. These include the power to investigate, the search by warrant, and the search and seizure without warrant, among others. Analysing the provisions contained in the Act reveals that they are in line with the general rules of the Criminal Procedure Code as detailed above including guarantees on the search of persons, the search of premises, and the search of suspected women (Section 77). In addition, the Act regulates rules relating to search and seizure without warrant over concerns of adversely affecting investigations or tempering with, removing, damaging or destroying evidence arising from any delay in obtaining the search warrant (Section 78). However, like the CPC, protection does not include all aspects of privacy but only that of personal and home privacy.

The DSA is equivalent to the US Electronic Records and Signatures in Commerce Act (or Electronic Signatures Act) of 2000 in that it gives electronic contracts the same weight as those executed on paper. The Malaysian legislation is different from the US with regard to privacy in criminal proceedings as it indirectly regulates criminal procedures related to digital signatures. No similar provisions are found in the US legislation which is fairly brief in nature.

The other cyber legislation in this category is the Personal Data Protection Act (PDPA) 2010 which was enacted in view of the large possibility of privacy invasion arising from advances in technology. Prior to its introduction, a sector-by-sector approach had been adopted in Malaysia for the protection of personal information through legislation, rules, regulations, codes or practice, and guidelines, among others, that were developed to govern and regulate the collection and use of information. These include those introduced in healthcare (Suhaila *et al.*, 2011) banking and financial institutions, insurance, etc.

The PDPA is a comprehensive legislation for regulating the process of personal data by data users in commercial transactions. It aims at preventing abuse relating to the storage and dissemination of information (Suppiah, 2010). In enacting it, Malaysia is said to have been influenced by the European Data Privacy standards (the EU Directive and the Council of Europe Convention 108) and two non-European privacy instruments, the OECD Guidelines and the APEC Framework (Greenleaf, 2012). The principles and rules under the PDPA are said to be influenced more by those in the European Union Data Protection Directive rather than those contained in the OECD Guidelines or the APEC Privacy Framework (Greenleaf, 2012). Thus, the PDPA does not adopt all the seven principles governing the OECD Guidelines, i.e., note, purpose, consent, security, disclosure, access, and accountability (Suppiah, 2010). The PDPA is hailed by Graham Greenleaf as the first of its kind in force in the region (Greenleaf, 2012). Sonny Zulhuda considers it a milestone for the development of electronic commerce and

electronic government in the country (Zulhuda, 2012). Likewise, Oan Seut Yen and Su Siew praise the legislation as a good start towards allowing the country to exercise rights to access, correct, control, and manage the use of the personal data by third parties (Oan and Su, 2010).

In addition, the PDPA makes a distinction between ordinary personal data and sensitive personal data, such as medical history, religious beliefs, and political opinions, which require explicit consent for processing (Wong *et al.*, 2010). Section 4 of the Act defines sensitive personal data as "any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data".

However, the statute has been criticized in being applicable only to the private sector or corporate bodies and to transactions of a commercial nature including banking, investment, financial services, insurance, to name a few (Kamal, 2011); (Kamal, 2012). Although the government is considered the main collector and holder of personal data, the statute does not provide for protection of privacy when it involves the public sector such as the federal and state governments, and law enforcement authorities (Zuryati, 2011); (Suppiah, 2010). In the words of Abu Bakar Munir, it is also limited to commercial activities that aim at profit and, as such, does not cover non-commercial activities, and non-profit activities (Abu, 2010). In addition, Oan Seut Yen and Su Siew Ling criticize this Act saying that it is not easy in some situations to draw a line between commercial activities including supply or exchange of goods and services and non-commercial ones (Oan and Su, 2010).

Moreover, the PDPA contains exemptions for many other activities including those by the media (Greenleaf, 2012). It also exempts from its scope of application protection against violation of personal data by individuals; (Zuryati, 2011) and obligations are imposed only on data users rather than data processors (Greenleaf, 2012). Further, the Act has also been criticized for not providing remedies for damages to breach of data subjects like the British Data Protection Act 1988 (Foong, 2011). The UK statute is said to have been the basis of Malaysia's PDPA (Zuryati, 2011). At the same time, the statute provides no clarification on what personal data collected before the date of its commencement compared with the Singapore law (Liau, 2013). Other drawbacks and limitations against the statute include its jurisdiction which is restricted to data processed only in Malaysia (Murni and Ratnawati, 2011); (Abu, 2010); (Kamal, 2011) among others (Greenleaf, 2012).

The other criticism is that the protection under the Act is limited to one aspect of privacy, that is, the informational or data aspect. As previously indicated, privacy is wider in its concept than the data which is deemed only one of the many aspects of this fundamental human right (Kamal, 2011). Other aspects of privacy such as personal privacy, family, and household affairs receive no protection in the statute (Abu, 2010). According to Lee A. Bygrave, this matter is one of the features of all privacy data laws. Data protection laws give relatively less importance to privacy as they strive mainly to protect other values and interests, and provisions of privacy in these laws is for the purpose of serving them (Bygrave, 2001). He likens this to the role of sustainable development policies, saying that data protection legislation seeks to protect privacy by protecting the interests of data controllers the same way in which sustainable development policies seek to preserve the natural environment (Bygrave, 2001).

This view is echoed by Jayaseelan who cited the then Minister of Energy, Telecommunications and Post of Malaysia as saying that tailoring and enforcing cyber laws in Malaysia enables MSC residents to achieve the full multimedia promise, and that without these laws the MSC as a comprehensive package will be incomplete and the growth of the multimedia industry will not take off (Jayaseelan, 1997). He opined that these legislations are also needed by the government in order to control cyberspace in observance of the public interests in coping with cyber offences (Jayaseelan, 1997).

Nevertheless, despite the above criticisms, the PDPA remains the most comprehensive legislation in the country in the area of information protection. In addition to commercial transactions, it also provides privacy protection in electronic government information transactions. The PDPA does not apply to federal government and

state governments (Section 3). According to Sonny Zulhuda, although it does not provide protection to the government as an entity, it still protects its activities. He argued that the Act is not applicable to government activities when they are undertaken directly by a public entity but applies only if they are carried out by a private entity (Zulhuda, 2012).

With regard to protection of privacy in criminal proceedings, the PDPA does this indirectly by regulating criminal procedures on personal data in Sections 112 to 127. These include the power to investigate (Section 112), search and seizure with warrant (Section 113), search of women (Section 113/5), search and seizure without warrant (Section 114), and access to computerized data (Section 115), among others. An analysis of the provisions contained in the Act reveals that they are also in line with the general rules of the Criminal Procedure Code in relation to the search of persons, premises, and suspected women.

The Payment Systems Act 2003 was introduced to make provisions for the regulation and supervision of payment systems and instruments, and for related matters. The Act provides regulations similar to the above-searched legislations in terms of the power to investigate clearing houses and powers of entry, search, and seizure (Sections 44 through 55). The regulations generally comply with those in the CPC and other legislations. The aim of the regulations, as indicated before, is to protect the privacy of individuals.

The Payment Systems Act is quite similar in scope to the US Right to Financial Privacy Act 1978 that protects the confidentiality of personal financial records. As with the PSA which protects privacy in criminal proceedings through search and seizure provisions, the RFPA requires federal government agencies to notify individuals and provide them the opportunity to object before a bank or other specified institution can disclose personal financial information to the agency.

3. CONCLUSION

The Malaysian legal system can be considered as providing no direct protection for privacy rights in the context of criminal proceedings. Such protection is provided indirectly in the Criminal Procedure Code as well as in other technology-based statutes especially in the area of cyber technology. Privacy rights also receive protection in provisions relating to criminal proceedings in some of the cyber laws of the country including the Computer Crimes Act 1997, the Digital Signature Act 1997, the Communications and Multimedia Act 1998, and the Payment Systems Act 2003. In addition, it receives similar indirect protection in the Personal Data Protection Act 2010 which is a major piece of legislation enacted specifically for privacy protection.

It can be concluded that the Malaysian legal system lags behind those of the developed economies in terms of provisions that address privacy issues in the collection of evidence in criminal proceedings. This is especially shown in the provisions of the Malaysian constitution which does not provide explicit privacy rights. It incorporates a due process clause that has received no agreement among scholars and practitioners as to whether or not it deals with privacy rights. While it can be argued that constitutional provisions do provide protection to privacy, they do not extend to areas involving criminal proceedings. Civil claims generally do not receive recognition on privacy as an actionable tort nor do they deal with criminal proceedings. As for the statutory framework, except for the CPC and some other sectoral statutes, most statutes make no reference to criminal proceedings. It is generally noticed that Malaysian cyber laws lack emphasis on the protection of privacy.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Contributors/Acknowledgement: All authors contributed equally to the conception and design of the study.

REFERENCES

Abu, B.M., 2010. The Malaysian personal data protection act: What it means for data users. MSC Malaysia Personal Data Protection Conference, Kuala Lumpur, Malaysia.

Abu, B.M. and H.M.Y. Siti, 2009. Electronic commerce legal framework: Some lessons from Malaysia. The Electronic Transactions Conference, Abu Dhabi, UAE.

Adler, M., 1996. Cyber-space, general searches and digital contraband: The fourth amendment and the net-wide search. Yale Law Journal, 105(4): 1093-1120. *View at Google Scholar | View at Publisher*

Barrera, M.H. and J.M. Okai, 1999. Digital correspondence: Recreating privacy paradigms. International Journal of Communication Law and Policy, 3(5): 4-9. *View at Google Scholar*

Beatty, D., 1998. Malaysia's "computer crimes act 1997" gets tough on cybercrime but fails to advance the development of cyberlaws. Pacific Rim Law & Policy Association, 7(2): 351. *View at Google Scholar*

Brenner, S.W. and B.J. Koops, 2004. Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1): 1. *View at Google Scholar*

Burgoon, J.K., 1982. Privacy and communication. CA: Sage Press.

Bygrave, L.A., 2001. The place of privacy in data protection law. University of New South Law Journal, 24: 277-283. *View at Google Scholar*

Duryana, M., 2012. Investigating cybercrimes under the Malaysian cyberlaws and the criminal procedure code: Issues and challenges. Malaysian Law Journal Articles. 6MLJi

Duryana, M. and R. Zulfakar, 2013. Cases of electronic evidence in Malaysian courts: The civil and syariah perspective. International Conference on Social Science Research, Penang, Malaysia.

Foong, C.L., 2011. Right to privacy in Malaysia: Do we have it? Malaysian Insider. (Malaysia, 21 Februari 2011).

Foong, C.L., 2012. Black day for internet users. Retrieved from http://foongchengleong.com/tag/evidence-act-1950/ [Accessed 18 January 2015].

Greenleaf, G., 2012. The influence of European data privacy standards outside Europe: Implications for globalization of convention 108. International Data Privacy Law, 2(2): 68-92. *View at Google Scholar | View at Publisher*

Ida Madieha, b.A.G.A., 2000. Digital technology, copyright and education the Malaysian perspective. 15th BILETA Conference: Electronic Datasets and Access to Legal Information, Coventry, England.

Jayaseelan, R., 1997. Policing cyberspace. New Straits Times (Malaysia), Aug. 16, 1997.

Kamal, H.H., 2011. Personal data protection in the business of higher education: Malaysian law' (2011) IPEDR. Singapore: IACSIT Press, 10: 55.

Kamal, H.H., 2012. Personal data protection in employment: New legal challenges in Malaysia. Computer Law & Security Review, 28(6): 696-703. *View at Google Scholar | View at Publisher*

Kirby, M., 1996. The impact of global media on the rule of law. Media Asia, 23(3): 123-137. *View at Google Scholar | View at Publisher*

Liau, Y.Q., 2013. Malaysia's data privacy act slow to take off. DZNet: 2. Retrieved from http://www.zdnet.com/article/malaysias-data-privacy-act-slow-to-take-off/ [Accessed 2 June 2014].

Lim, K.S., 1997. Speech-digital signature bill. 4. Retrieved from http://www.limkitsiang.com/archive/1997/May97/sg389.htm [Accessed 7 February 2015].

Murni, W.M.N. and M.A. Ratnawati, 2011. Technology and the deterioration of right to privacy. International Journal of Asia Pacific Studies, 7(2): 35-50. *View at Google Scholar*

Nazura, A.M. and T. Hossein, 2012. Cyber crimes: Lessons from the legal position of Malaysia and Iran. International Journal of Information & Electronic Engineering, 2(3): 404-408. *View at Google Scholar | View at Publisher*

Oan, S.Y. and S.L. Su, 2010. The Malaysian personal data protection Act 2010: A brief overview. Tay & Partners. Retrieved from http://www.taypartners.com.my/en/images/OurResources/Articles-LegalTaps/legaltaps-201008.pdf [Accessed 22 January 2015].

Prins, C., 2007. E-government: A comparative study of the multiple dimensions of required regulatory change. Electronic Journal of Comparative Law, 11(3): 1-23. *View at Google Scholar*

Ranjan, P.S., 1997. Telemedicine Act 1997. Cyberlaws in Malaysia Seminar, Kuala Lumpur, Malaysia, November 1997.

Sangal, P.S., 1997. Malaysia creates legal infrastructure for its multimedia super corridor. International Company and Commercial Law Review, 12: 428-430. *View at Google Scholar*

Siddiqi, M.Z., 1999. Cyberspace crimes: The Malaysian experience. Voice & Data, Guest Column. Retrieved from http://www.voice~data.com/jul99/guest%5Fcolumn1.html [Accessed 28 December 1999].

Suhaila, S., A. Rabiah and I. Zuraini, 2011. Towards implementing a privacy policy: An observation on existing practices in hospital information system. Journal of E-Health Management. Retrieved from http://www.ibimapublishing.com/journal/JEHM/jehm.html [Accessed 25 January 2015].

Suppiah, R., 2010. Awakening to a new dawn-the personal data protection act 2009. Malaysian Bar. Retrieved from http://www.malaysianbar.org.my [Accessed 22 January 2015].

Wong, A.A., K.K. Wong and A. Martin, 2010. New data law in Malaysia. Baker& McKenzie. [Accessed 29 May 2013].

Wong, C.Y., 2002. Malaysian law and computer crime. SANS Institute. Retrieved from http://www.sans.org/reading-room/whitepapers/legal/malaysian-law-computer-crime-670. [Accessed 14 January 2015].

Zaharom, N. and K.A. Mustafa, 1998. IT strategies in Malaysia: The Multimedia super corridor. UNRISD Conference on Information Technologies and Social Development, Geneva, Switzerland.

Zinatul, Z.A., 2000. Electronic commerce: A comparative analysis of the Malaysia digital signature act 1997 and the Singapore electronic transaction act 1998.15th BILETA Conference: Electronic Datasets and Access to Legal Information. Coventry, England, 2000.

Zulhuda, S., 2012. The state of e-government security in Malaysia: Reassessing the legal and regulatory framework on the threat of information theft. ICCIT. Retrieved from http://irep.iium.edu.my/27226/1/E-government_%26_Info_Security_print_for_proceedings.pdf [Accessed 23 January 2015].

Zuryati, M.Y., 2011. The Malaysian personal data protection act 2010: A legislation note. New Zealand Journal of Public and International Law, 9(1): 119-135. *View at Google Scholar*