Journal of Politics and Law; Vol. 12, No. 1; 2019
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Modern Means of Evidence Collection and their Effects on the Accused Privacy: The US Law

Adam Mohamed Ahmed Abdelhameed[1] & Kamal Halili Hassan[2]

[1] United Arab Emirates Embassy, Seoul, South Korea

[2] Faculty of Law, Universiti Kebangsaan Malaysia, Bangi, Malaysia

Correspondence: Kamal Halili Hassan, Faculty of Law, Universiti Kebangsaan Malaysia, Bangi, 43600, Selangor, Malaysia. E-mail: k.halili@ukm.edu.my

Received: January 2, 2019 Accepted: February 22, 2019 Online Published: February 28, 2019

doi:10.5539/jpl.v12n1p85 URL: https://doi.org/10.5539/jpl.v12n1p85

Abstract

The objective of this article is to discuss modern means of evidence collection by the enforcement agencies and their effects on the accused privacy under the United States' law. Focus of this article is on the modern means of evidence collection such as electronic surveillance, wiretapping and technology eavesdropping, among others. In the age of modern technology, the objective of revealing the truth and instituting justice has encouraged those with an interest in matters of criminal justice to use modern means beside or instead of the conventional means of evidence collection. Resorting to modern means is premised on the need for criminal proceedings to reflect the circumstances and level of progress of the society where it has been taken. The main problem here however is that there is a possibility of the law enforcement interest in prosecution to be favored and the accused rights to be underrated. We found that at the US federal level, the accused's privacy right is one of the rights included in the Bill of Rights in 1791 (Fourth Amendment) and supported by many case-law. The article adopts a legal analysis approach which is an accepted form of a qualitative method in social science research.

Keywords: privacy right, US law, criminal investigation and proceedings, modern means of evidence collection

1. Introduction

Human rights and fundamental freedoms are recognized in all legal systems (Yaakob 2016; Hassan & Ismail 2016; Hassan et al 2018). Within the context of the criminal justice system, almost all jurisdictions provide rights for the accused person as part of the said rights and freedoms in order to enable him or her to defend him or herself (Safavi & Syukur 2014). These rights are considered the core idea behind thinking of human rights in the criminal proceedings. Although they are generally known as rights, they might be provided in other forms such as freedoms, presumptions, principles, rules or privileges, among others. While these rights might be spelled directly in some legal systems, they might be indirectly derived as a result of interpreting the spelled ones or being practiced as civil claims. In many cases, the accused person is set free not because he or she is innocent but because the law enforcement agencies do not observe the above-mentioned rights (Thompson 2006).

Against the said rights and freedoms including the right to privacy, there is an interest in evidence collection considered to be decisive in the investigation of offences and prosecution of offenders in criminal proceedings (Hassan 2012). This interest has resulted into granting law enforcement agencies the power to undertake what might lead to its achievement. The legal system in a certain jurisdiction, i.e., the constitution, federal legislations, by-laws, case laws and local regulations, bestows law enforcement agencies with the authority to prosecute the offenders, i.e., the persons accused of breaching the social order, disturbing the public morality, destabilizing security or infringing on the rights and/or freedoms of other persons. These agencies are entrusted with exceptional powers in the performance of the above-mentioned assignment. Powers given to these agencies include carrying out thorough investigation, search and seizure and arrest and detention of the suspected person, etc., in order to gather the evidence. The fundamental consideration when deciding to prosecute or not is whether doing so would be in the interest in evidence collection. That is because a prosecution should be initiated or continued, subject to the availability of evidence that discloses a *prima facie* case, if it is in the interest in evidence collection, and not otherwise. This article discusses the legal position of such issue in the context of the United States legal system.

2. Methodology

The methodology for this research/article is qualitative. A doctrinal-type of research is used based on secondary library materials including statutes, decided cases, books and journal articles on the topic. The data analysis was performed through a content analysis of the said secondary data to obtain the findings. Provisions of the statutes in operation and court cases in the US are analysed for the purpose of exploring the areas in which the accused person's right to privacy is not adequately valued vis-à-vis the interest in modern evidence collection as well as to assess if the latter is balanced with the former. In addition, scholarly works related to this matter were also reviewed and critically discussed. This is a purely legal study which is primarily based on legal analysis. Hence, there is no field work such as questionnaire survey or interviews carried out.

3. Results and Discussion

3.1 Modern Means of Evidence Collection

The evidence obtained by or through these means and devices is admitted in courts proceedings for revealing the truth, as an alternative to the primitive ordeals used in medieval ages that invade the dignity and worth of the human being (Lederer 1984). This is shown in a landmark decision made by the American Federal Court in the *Daubert v Merrell Dow Pharmaceuticals, Inc.* case in 1993. In this case, the plaintiff sued the defendant claiming that a prescription drug marketed by the defendant for maternal use had caused birth defects of her children. The Court asked for a testimony from an expert. Based on the testimony, the Court unanimously ruled in favour of the admissibility of the scientific evidence in the court (Majmudar 1993). According to Orofino (1996), the *Duabert* verdict resolved a long debate about the admissibility of scientific evidence in court proceedings and offered an optimistic vision of how science and law could cooperate in the resolution of conflicts in the courtroom.

Modern means referred to by law enforcement agencies include wiretapping, eavesdropping or electronic surveillance, among others. Various modern listening devices could be unobtrusively attached to a telephone, tiny match-head transistors that could be fitted into a cocktail olive or be concealed in a lamp or car upholstery. They could be adapted to the fillings of a tooth, embodied in a denture or masqueraded as wristwatches or fraternity pins. Stethoscope microphones could be applied to the wall by suction or driven into a party-wall as spike (Madgwick & Smythe 1974).

It is technically possible for details about one's life, such as family circumstances or financial situations to be recorded in a central computer with any of the information being made available to anyone who might ask for it including law enforcement agencies. In the cyber age, messages exchanged between users that are stored in the system could be reviewed and publicized by operators. Such messages include the ones in the addressee's mailbox waiting to be picked up and records of private discussions between users, instant messaging, chat, non-voice file transmission, social networking, blogging, sharing of images and movies, web browsing, etc. According to Jesdanun (2001), these uses of the internet create challenges to privacy that require to be addressed. Data seized from one's activities in cyberspace might be used in the criminal justice field in one of the interconnected operations of the law enforcement agencies, including the police and prosecution. Secret seizure of e-mails and online communications stored in computer files, hard disks or other related materials of a person suspected of committing an offence in search of evidence might violate the right to privacy.

3.2 Evidence Collection v. Privacy Right

From the above discussion, there are two sets of interest: the individual's interest in protecting his or her right to privacy if he or she is found to be subject to search or seizure in criminal proceedings and the law enforcement interest in evidence collection. The good legal system is the one that manages to maintain a balance between the two sets of interest. Requiring the warrant for law enforcement agencies to conduct the search or seizure means recognizing the individual's privacy right without ignoring, at the same time, the law enforcement interest in prosecuting offences. However, conducting the search or seizure without such a warrant might be regarded as a violation of one's privacy right as this procedure might expose the person's personal information, while giving priority and supremacy to the public interest in prosecution.

Criminal procedure legislations are in place to safeguard innocent people and punish the wrongdoers as a means for the protection of the individuals being the basis for society, not only as a means for punishment. In other words, criminal procedure codes are mechanisms that aim at achieving the respect and protection of the rights of the criminally accused persons and the coexistence of these rights with the law enforcement interest in prosecuting offenders and inflicting punishment upon them. The rules and principles articulated in criminal procedure codes are designed to mediate between the need to effective law enforcement and the need to protect

rights and liberties of the individuals in the criminal justice.

The interest in evidence collection and the private rights of the accused person are there to co-exist in the process of evidence collection without giving one of the two sets of interest priority or supremacy over the other. However, in some situations the private rights of the accused might be undervalued for the purposes of the interest in evidence collection. The public right to seek the truth and to establish justice as part of the justifications behind the public prosecution could be overvalued at the expense of the rights of the accused persons as the process of prosecution might result in the accused persons' rights to be infringed by law enforcement agencies.

Thus, the main problem here is that there is a possibility of the law enforcement interest in prosecution to be favored and the accused rights to be underrated. That is to say, the law enforcement agencies might breach the rights of the accused persons while these agencies perform their duties in evidence collection. In other words, the observance of the law enforcement interest in the prosecution of offences might lead to the violation of the rights of the accused person. In the words of a Gihad (1991), there are two considerations that dominate the evidence collection in criminal proceedings. The first is the keenness for more effectiveness in the search of the truth that might leads to violation of the accused's rights. The second is the willingness to protect the said rights that might result in some situations in the failure of the justice system in prosecuting the offender. According to McHarg (1999), the conflict between the interest in evidence collection and the accused rights might take place when each of the two sets of interest is observed to its greatest extent without taking into account the other.

It follows from the above that the privacy right as one of the rights of the accused person could be violated in situations where the law enforcement agencies conduct some proceedings to gather the information and evidence about a committed offence and the offender. In the words of Awade (1988), from the moment an offence is committed, two sets of interest compete: the first is the basic rights of the suspect including his or her privacy and the other is the public interest in the prosecution of the offender. A similar point of view is echoed by Reinert (2010) who stated that American courts perceive the disputes related to the Fourth Amendment as a conflict between the law enforcement interest in evidence collection and the rights of the suspects including the privacy right. According to Hong (2011), in many situations the observance of the interest in evidence collection could influence the right to privacy as the former might be given more weight at the expense of the latter. In decided cases, the need for balancing the law enforcement interest in evidence collection with the privacy right of the accused is highlighted in the *Wyoming v Houghton* (1999, 526, U.S. 295) that addresses the constitutionality of conducting a warrantless search of a container under the "automobile exception" to the Fourth Amendment's warrant requirement. In writing the opinion of the Court, Justice Scalia stated that the starting point in determining whether or not the privacy right of the accused is violated for every case that involves search and seizure is a modern balancing test if the common law under which the Fourth Amendment was framed yields no answer.

In addition, as this matter at issue takes place in the process of the conventional means of evidence gathering such as the search of persons and of premises, it might also occur when the said agencies utilize modern means for the purpose of evidence collection. Examples to these means include interception of telephone calls of the accused, tracking his or her online communications and accessing his or her computerized data. As put by Bellia (2004), in allowing the evidence collection through electronic surveillance the American Congress is led to believe that the law enforcement interest in evidence collection could be overvalued and the privacy right as one of the rights of the accused person could be undervalued. She opined that less attention was given to the normative principles that guide the Congress in balancing the law enforcement interests in evidence collection with the privacy right of the accused. In discussing the exemptions in technology-based statutes given to law enforcement agencies in the evidence collection versus the privacy of the accused, Murphy (2013) opined that the interest in evidence collection dominates.

3.3 Implications of Modern Means: The United States' Law

Against the backdrop of the success of the technological advancement in the different fields of our lives, law enforcement agencies in criminal investigation have resorted to technological devices for more efficiency in gathering the evidence about a committed offence and the possible offender. Hence, listening devices are used to overhear suspect's telephone conversations with other people. Calls made by a suspect are intercepted through installment of devices to his or her home, office, car or even public places such as public telephone booths (Craigs 2007). Surveillance and tracking devises such as the global positioning system (GPS) as well as pen registers and other traps and track devices are used for the same purpose. In addition, a respondent's personal computer or other data storage media were seized and searched for evidence against him or her. The suspect's

e-mail account and his or her online activities such as the ones in social media or chat rooms were tracked by law enforcement officials for the purposes of evidence collection. Moreover, DNA analysis, thermal imaging and aerial imagery and surveillance were also employed in criminal investigations. All the above-mentioned technologies were used in the experience of the American law enforcement agencies. With the recent progress made in artificial intelligence (AI), attention is also growing over the possibility of the incorporation of the AI into criminal investigations especially in cyber-crimes (Dileks et al 2015; Alzou'bi et al 2014). These have raised questions and controversies with regard to the implications of their use for evidence collection purposes on the suspect or accused's privacy right similar to the ones raised with regard to the search and seizure executed by law enforcement officials in its conventional form. The problem with these new technologies is that they are used for evidence collection purposes before the introduction of the legal framework that regulates their use (Birell 2015).

As with the conventional means of evidence collection, the American Federal Constitution is also referred to regarding the implications of the use of modern means in criminal investigation on the accused person's privacy. Rule 41 is also a source of reference as it encompasses the contents of the warrant including the particularity test with regard to the place to be searched and the date and time for the execution and return of the warrant. In addition, privacy is addressed in a number of technology-based statutes. Media-related privacy is regulated by the Cable Communications Policy Act that deals with the cable industry and the Electronic Communications Privacy Act that regulates government officials' authority to intercept or obtain information available electronically such as the one in e-mails or internet service providers (ISPs) logs and public library patron records. Likewise, there are also statutes that regulate personal information privacy related to videotapes, telephone consumers, telecommunications and children online. These include the Videotape Privacy Protection Act, the Telephone Consumer Protection Act, the Telecommunications Act 1996, the Children's On-line Privacy Protection Act 1998 (COPPA), the Video Voyeurism Prevention Act (VVPA) 2004 and the Telephone Records and Privacy Protection Act (TRPPA) 2006.

According to Levin and Nicholson (2005), the American Constitution and its supporting body of jurisprudence do not provide adequate protection to privacy against the continuing advancement of technology. They argued that this is because reasonable searches and seizures by the government are permitted under the Fourth Amendment. In addition, no expectation of privacy is guaranteed as a requirement for protection in public spaces in which modern technological devices such as video cameras can be installed for recording people's images and personal locators like global positioning systems (GPSs) through which one can be tracked. In defending privacy against the use of new technologies for evidence collection purposes, Birrell (2015) called for adopting measures that discourage this use including monetary compensation for privacy invaders together with establishing the minimum level of expectation of privacy.

This required us to explore the possible implications of modern technological means of evidence collection on the accused person's privacy. Following would be a discussion of the above mentioned means and technologies used in evidence collection. These include electronic surveillance, wiretapping, eavesdropping, pen registers and trap and trace devices, search of computers and storage media, monitoring of electronic communications, analysis of DNA samples, thermal imaging and aerial imagery and surveillance. It should be mentioned here that the discussion would highlight the legal framework that regulates the use of each means or technology. This is because the statutes listed above tend to address technology-based concerns as each statute deals with the activities related to a certain technology as the titles of the statutes suggest. In other words, the statutes were enacted in response to the invasion upon privacy through the usages of the said technologies (Murphy 2013).

3.4 Electronic Surveillance

According to Dawn Webber, at the beginning of the use of electronic devices in surveillance, the American Supreme Court rejected the claims of privacy intrusion on the grounds that the intrusion that violates the Fourth Amendment in criminal investigation should be a physical one (Weber 1984). That is to say, the Court required the intrusion to be through a civil claim trespass onto a constitutionally protected area or private property in order for it to meet the constitutional meaning of the search intended by the framers (Bellia 2015). This was emphasized in the *Olmstead v United States* case in 1928 that involves wiretap by law enforcement officials, as explained earlier, in which the Supreme Court rejected defendants' challenge for not meeting the trespass test in a ruling that shows Justice Brandies' dissent judgment. In other words, it concluded that unwarranted listening does not represent search in a constitutional sense as law enforcement officials did not physically trespass on the defendant's property. A similar conclusion was also reached in subsequent cases including the *Goldman v United States* case in 1942 and the *Berger v New York* case in 1967, as detailed earlier. At the same time, the use of such means by law enforcement officials continued to be controversial (Winn 2008).

The Court, however, changed its position in the same year in the *Katz v United States*, when law enforcement officials listened to the conversation through a listening and recording device installed to a public telephone booth, in which it ruled that the Fourth Amendment protects people not places against unreasonable searches and seizures as long as the individual has a reasonable expectation of privacy. This means the ruling has eliminated the physical trespass element from the Fourth Amendment. The presence or absence of physical intrusion on a constitutionally protected area is no longer given weight in defining the search and seizure based on this ruling (Bellia 2015). The ruling has also given recognition to the invasion through modern means as well as rejected the admissibility of the evidence collected in violation of privacy (Weber 1984). The *Katz* is criticized for the weaknesses of its reasoning as, among other things, it mixed between the subjective and objective criteria in the reasonable expectation of privacy in saying that the person should exhibit an actual subjective expectation that society is prepared to recognize as reasonable (Harper 2008). Nevertheless, the *Katz* formula is praised for holding special significance as it extended beyond the boundaries of the Constitution and found its way into civil claims, statutes and laws of other countries. In addition, it formulated the objective test for reasonable expectation of privacy based on the average person (Winn 2008).

In response to these cases, the American legislator enacted Title III of the Omnibus Crime Control and Safe Streets Act (Title III) in 1968 to regulate surveillance activities. In this Act, surveillance activities were prohibited and criminal penalties and civil damages were provided against those, law enforcement officials or private parties, who intercept, endeavor to intercept or procure any other person to do so. However, Title III is criticized for not satisfying all the requirements of the Fourth Amendment as it does not require the particularity test with regard to the place to be searched and the persons or things to be seized in the interception warrant (Bellia 2015).

It should be mentioned here that law enforcement agencies collect information electronically under the regulations of the Electronic Communications Privacy Act (ECPA) 1986. The Act provides protection to wire, oral, and electronic communications while in transit, and communication held in electronic storage. The ECPA sets the requirements for search warrants under some circumstances that are more stringent than in other settings. The Act also bans government and law enforcement agencies from monitoring messages sent via public electronic mail. It also outlaws the use of devices to record dialling, routing, addressing, and signalling information used in transmitting wire or electronic communications without a search warrant. However, it contains provisions that allow disclosure on the basis of a simple administrative request of law enforcement agencies (Murphy 2013). In addition, it contains many exemptions to the general rule that forbids interception of electronic communications (Overton & Giddings 1997). The ECPA amended Title III to prohibit not only the interception of wire and oral communications but also the interception of electronic communications. The Act comprised three statutes: the Wiretap Act, the Stored Communications Act and the Pen Register Act. Distribution of ECPA regulations among the three statutes comes in recognition of three categories of communications, i.e., wire communications, oral communications and electronic communications (Bignamy 2015).

3.5 Wiretapping

The Wiretap Act is referred to in the intercept of the content of the communication by law enforcement agencies at the time when the communication is taking place. Prosecutors refer to this procedure through showing the court that there is a reasonable cause to believe that a criminal offence has been committed for them to obtain an order from the court to intercept the communication. Here, the targeted person should receive notice about the surveillance in 90 days after its completion. The Act applies to wire and oral communications rather than to other means of communications (Bignamy 2015).

Title III exempts law enforcement officials from its general rule that forbids interception of wire, oral and electronic communications if there is a court order, consent of one of the parties to the communication or an intruder to the communication system. The application of the court order should be approved by a senior official from the Justice Department upon a showing of probable cause to believe that the interception would produce an evidence of a federal offence or the whereabouts of a fugitive fleeing from prosecution of such an offence. Title III also sets the conditions for the uses and disclosure of the information collected from the interception based on the consent of the party to the communication whereby it is required to be freely given with no regard to whether be explicit or implicit (Doyle 2012).

In the words of Erin Murphy, the enactment of Section 605 of the Federal Communications Commission Act is considered the critical point in privacy protection against wiretapping, as the American Supreme Court ruled in favour of the prohibition of wiretapping based on its interpretation of the Section (Murphy 2013). Here, the *Katz v United States* is worth mentioning. In this case the American Supreme Court ruled that wiretapping of the

telephone conversation in a public telephone represents a search under the Fourth Amendment as it violates Katz's reasonable expectation of privacy. According to Lisa Schmidt, this ruling is in line with the principle that any activity that is not considered a search does not receive constitutional privacy protection as the protection under the Fourth Amendment is limited to unreasonable searches and seizures (Schmidt 2012).

3.6 Eavesdropping

Eavesdropping involves usage of radio receiver to overhear a cordless-telephone conversation. It requires a warrant under the federal wiretapping statute, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Sklansky 2015). Eventually, the American Supreme Court made a compromise in the famous case, *Katz v United States (1967),* with regard to eavesdropping. It made eavesdropping constitutionally permissible, in condition that it is based on a warrant showing the probable cause.

As for the implication on privacy in criminal investigation at the state level, yet the principal prosecuting attorney of a state or any of its political subdivisions is granted the authority to approve an application for an order used for wiretapping or electronic eavesdropping. The only required condition here is that the agency seeking the order should show that there is a probable cause to believe that the interception would produce evidence of a felony under the state laws covering offences including murder, kidnaping, gambling, robbery, bribery, extortion, drug trafficking, or any other crime dangerous to life, limb or property (Doyle 2012).

3.7 Pen Registers and Trap and Trace Devices

Pen registers record the numbers called from a particular instrument while trap and trace devices identify the sources of incoming calls as they record these numbers (Sklansky 2015). The use of pen registers and trap and trace devices is regulated by the Pen Register Act. Installation and use of a pen register or trap and trace device is not allowed for criminal investigation without a court order. Here, law enforcement agencies should show the court that the information is likely to be collected through the installation of a device for recording the numbers called from a particular instrument for pen registers or identifying the sources of incoming calls for trap and trace devices in order for the court to issue the order for the installation of the device. In other words, law enforcement officials are required only to certify that the information is relevant to an on-going criminal investigation without any additional explanation of this relevance for them to have the court order issued for the above-mentioned purposes. Thus, this legislation allows easy invasion of privacy through the simplification of the safeguard requirement. Compared with what is provided in both the Wiretap Act and the Stored Communications Act, the person subject to the surveillance under the Pen Register Act in not required at all to be notified about the installation of the device (Bignami 2015). However, recording of the numbers by pen registers and trap and trace devices are not considered interception under Title III as they do not allow the user to overhear the contents of the telephone conversation or capture the contents of the communication (Doyle 2012).

The Supreme Court ruled in the *Smith v Maryland (1979)* that the Fourth Amendment does not extend to the government's use of pen registers and that the installation and use of pen registers was not a search within the meaning of the Fourth Amendment and hence no warrant was required. In this case, the Court faced the question of whether a placement of a pen register on the suspect's telephone line without warrant violated the Fourth Amendment (Harper 2008). Reasons cited for not extending Fourth Amendment protection to pen registers include the pen register's limited capability and partiality of the information obtained from it. Thus, the use of pen registers has been deemed less intrusive in privacy as compared to wiretapping, for instance (Friess 2012). According to Jim Harper, in this case the American Supreme Court again returned to its previous position that relied on the trespass of the premises due to the weaknesses of the *Katz* (Harper 2008).

3.8 Search of Computers and Storage Media

The Fourth Amendment rules on search and seizure in conventional means in criminal investigation were also extended to the search and seizure of computers and storage media through the translation of physical world rules to the information stored in a computer or a storage medium. Here, the established rules in examining objects in the physical world such as drugs, clothing or blood, were fitted to computer forensics. (Goldfoot 2011) The American Supreme Court ruled in the *United States v United States District Court* that besides the physical invasions of privacy, the Fourth Amendment also protects privacy against nonphysical invasion. It also ruled in the *United States v New York Telephone Co.* that Rule 41 of the Federal Rules of Criminal Procedure is not limited to tangible items but flexible to include within its scope electronic intrusion.

This approach is criticized by Orin Kerr for not meeting the special nature of the computer search and seizure in which the process of search and seizure is divided into two steps. At the first step, a physical search to seize the computer itself is conducted. In the second, another search is executed to collect data from the seized computer

as digital evidence (Kerr 2005). He argues for the need of the warrant process to be revised to take into account the two steps of the search and be put into one step. In addition, it should also meet the search particularity test in which general constitutional and statutory rules of physical search are used. He called for the warrant to include particularity with regard to the second step in which a digital evidence is collected. He proposed a one warrant that contains details for both steps of the search and seizure. There is also disagreement as to whether storage media are distinguished from other objects such as closed containers. Distinction between the two is found in the *State v Smith* (2009) in which the Ohio Supreme Court required the warrant for searching the contents of the cell phone. The other position is found in the ruling by the California Supreme Court in the *People v Diaz* (2001) in which it rejected a distinction between the cell phone and its contents.

According to Goldfoot (2011), the disagreement between the positions of the two rulings is based on the nature of the data, whether it is a thing or not. Applying physical world rules to storage media including computers is premised on the container and sub-container perspective. Directories, folders and files of the computer each is considered a separate container that requires a warrant specifying particular description of the category to be searched or seized similar to things in the physical world. However, the container perspective is criticized for facing some practical problems and shortcomings with regard to the requirements under search and seizure including the particularity of the place to be searched and persons or things to be seized, among others, as the search of all data is like a search that includes all the objects in a house in the physical world. In the *United States v Carey (1999)*, for instance, a federal circuit court excluded the evidence resulted from a computer search due to the expansion of the scope of search to image files not mentioned in the warrant in violation of the Fourth Amendment. It also raises problems in relation to what is meant by the search and seizure and when each should happen as well as the rules that govern the jurisdiction, execution and reasonableness.

With regard to whether or not the expectation of privacy in the computer information is assessed based on the premises-based test that relies on what the person seeks to keep private, a recent decision by the Supreme Court affirms the latter. In the *United States v King* (2007) that involves access to defendant's computer by a military computer specialist and discovery of pornographic materials, the Court of Appeals for the Seventh Circuit applied the *Katz* doctrine and concluded that King's computer files do not enjoy Fourth Amendment reasonable expectation of privacy protection. The reason behind this decision is that the files in question were considered part of the military network and then exposed to everyone with network access (Harper 2008).

For the search of digital information on cell phones, the Supreme Court required a search warrant in a recent ruling. It ruled in the *Riley v California* case (2014), that a warrant is generally required to search digital information on a cell phone seized pursuant to an individual's arrest. It should be stated here that based on the ruling in this case a proposal is made for a reasonable legislative that makes a balance between the interest in evidence collection and the privacy interest of cell phone owners through the warrant requirement, but no action was taken (Sklansky 2015).

3.9 Monitoring of Electronic Communications

In addition to the above-mentioned means, law enforcement agencies monitor electronic communications for collecting evidence in the criminal investigation. The Stored Communications Act (SCA) regulates the records of the electronic communications services such as e-mail accounts, electronic bulletin boards, voice mails, pagers and remote computing storage service providers that cover outsourced storage and processing services commonly known as cloud (Bignami 2015). It was enacted as a statutory version of the Fourth Amendment for computer networks (Friess 2012). The SCA protects one's privacy contained in his or her e-mail accounts and other online activities. It bans invisible access to communications at rest (Doyle 2012). The statute addresses the collection and monitoring of routing information in storage such as contents of e-mails, metadata such as e-mail senders and receivers and records of subscribers including their names, addresses and method of their payments to the service provider, text messages, and the archiving of telephone records that pen registers and trap and trace devices previously collected much more selectively (Sklansky 2015).

Under the SCA, law enforcement officers are required to obtain a court order before conducting the search and seizure in observance of the privacy of the e-mail holder. The court order allows law enforcement officers to access all the e-mails in storage of the subscriber's information and contents for more than 180 days, except for the ones that have not been accessed, viewed or downloaded. In this situation, the person in charge of executing the search and seizure should access only the message or messages related to the offence for which the court order was issued in the belief that the e-mail contains its evidence (Bedi 2014).

However, law enforcement officers may access the entire messages regardless of whether they are related to the offence for which the court order was issued or other ones containing personal information (Friess 2012). In

addition, internet service providers (ISPs) are not allowed under the Act to notify the subscriber of accessing his or her e-mail account. Compared with the Wiretap Act, the SCA does not restrict the use or dissemination of the information for other law enforcement purposes (Bignami 2015). Nevertheless, invasion of privacy is possible despite the guarantees provided to the stored communications as the Act allows courts' orders for wiretapping or electronic eavesdropping (Doyle 2012). Here, the protection provided to privacy under this legislation is not adequate as the statute does not require a warrant for the search and seizure whereby other requirements should be met. These include the establishment of probable cause to believe that the search of the stored e-mails would uncover an evidence of an offence, limiting the search to e-mails related to the offence in question and limiting the search and seizure to e-mails sent or received during the time when the alleged offense is committed (Friess 2012).

While agreeing that internet social networks do not receive Fourth Amendment protection due to the absence of reasonable expectation of privacy or the consent search through privacy policies and rules, Schmidt (2012) calls for extending the Amendment protection to the activities and relationships that users seek to preserve as private in these networks even in an area accessible to the public. The same position is echoed by Bedi (2014) as saying that the internet embodies the same principles of traditional autonomy activities and ties that focus on developing intimate life with others such as sharing with them personal thoughts, experiences and beliefs thus they should receive constitutional protection. This can be done through the usage of the mosaic doctrine developed in the area of government surveillance of public movements that relies on third party doctrine on societal reasonable expectation of privacy. The doctrine allows law enforcement officials to access the records or transactional data of someone other than the suspect such as his or her cell phone service provider without warrant or constitutional search under the Fourth Amendment. This is supported by court verdicts as the Supreme Court concluded in the *United States v Miller* (1976) that law enforcement agencies' access to a third party, a bank record, is not deemed a search. The Court also reached a similar verdict in the *Smith v Maryland* (1979) that involves access to telephone metadata of the service provider.

The expectation of privacy in e-mail messages is not reasonable viewed from the perspective of the society for three reasons. The first reason is the e-mail holder's inability to control the message once it is transmitted as the recipient may forward, print or disclose the message. The second reason is the user's reliance on a third party such as the service provider. The last reason is the vulnerability of the messages by hackers. The doctrine is defended by some scholars among them is Orin Kerr who argued in favor of its applicability in criminal investigation to fill the shortcomings left by the constitution, which in his view, allows phantom of privacy threats to block necessary criminal investigative steps (Kerr 2005). Bambauer (2015) calls for the revision of the doctrine in order to protect the subjects of criminal investigations from the harm of law enforcement discretion without causing unnecessary conflicts with other societal interests beyond the interests of the criminal such as the due process interests of the criminal suspects, equal protection and freedom of speech. According to her, this closes the exploitative uses of third party record by law enforcement officials.

The provisions of the SCA is in harmony with the search and seizure requirements provided in the Fourth Amendment and called for the revision of the statute to include the warrant. She argues that e-mails are more intrusive compared to wiretapping and video surveillance because e-mails usually contain several aspects of personal information than phone conversations or video recordings as each contains only one aspect. According to Friess (2012), the Fourth Amendment stands as the constitutional factor between the governmental need in investigating offences and societal need to safeguard privacy of the individuals. Courts also concluded that the Fourth Amendment should keep pace with the unseen technological progress. This has been applied to the telephone conversations and video camera surveillance. In the *Katz v United States*, the Supreme Court required implementation of Fourth Amendment requirements, which used to center on the property to telephone wiretapping in non-residential premises. Likewise, the Court also extended the same ruling to video cameras in the *United States v Torres* on the grounds that both wiretapping and surveillance share in common been unseen by the victim.

Regarding how the reasonableness in the monitoring of electronic communications is determined, the Supreme Court held in the *Terry v Ohio* (1968) that reasonableness is defined through balancing the needs of the government to search or seizure against the invasion made as a result of the search or seizure. This is decided through a combination of rules and presumption of the Fourth Amendment designed to control the conduct of law enforcement officials who may invade privacy. In other words, for law enforcement officials to secure a warrant before conducting the search and seizure, officials are required to justify the need for the search and seizure through establishing probable cause and particularity.

3.10 Analysis of DNA Samples

The other modern means used in criminal investigation in the collection of evidence is the analysis of DNA samples. The abandoned DNA samples are employed against some suspects to show a connection between a suspect and a committed offence raises question with regard to the reasonable expectation of privacy (Levin & Nicholson 2005). Law enforcement agencies claimed that if someone leaves his or her DNA sample behind, he or she cannot expect it to remain private. They analyzed abandoned DNA samples in search of evidence without a warrant. The use of genetic information resulted from the DNA analysis is analogized to the trash based on the verdict by the American Supreme Court in the *California v Greenwood* in 1988. In this verdict, the Court held that the defendants had no expectation of privacy in the trash bags they left on the roadside, hence anything that is abandoned can be searched without a warrant.

Privacy advocates argued that DNA samples are different from trash and that they contain much more personal information compared to trash. In addition, they said that the person should enjoy reasonable expectation of privacy for his or her DNA samples as it is impossible for anyone to avoid leaving behind his or her DNA sample. So far, the American Supreme Court heard no case in order to uphold or reverse this analogy. However, state courts such as in Nebraska ruled in favor of law enforcement position. In the *State v Wickline* in 1989 and the *State v Buckman* in 2000, the Nebraska Supreme Court held that abandoned DNA sample is analogous to abandoned trash, thus it does not enjoy Fourth Amendment protection that requires a warrant. In the two cases, the evidence through genetic information was collected from the analysis of the DNA samples left by the respondents in cigarette buffs seized by law enforcement officers.

3.11 Thermal Imaging

Thermal imaging devices are also used in evidence collection in criminal investigation. Early rulings likened thermal scanning to abandoned trash similar to what we have discussed in the analysis of DNA samples on the grounds that thermal radiations or heat waves are allowed to leak out private premises to public space and then it can be observed by anyone who uses a thermal scanner. Examples are the *United States v Pinson* in 1994 and the *United States v Ford* in 1995. However, the recent famous *Kyllo v United States* ruling in 2001 reversed the situation. It was held that thermal scanning requires a warrant and probable cause based on the Fourth Amendment (Solove & Schwartz 2015). Against the backdrop of suspecting Kyllo of growing marijuana in his house using high-intensity lamps, law enforcement officials in this case used thermal imager whereby a heat was detected over the roof of the garage and on a side wall of the defendant's house compared with other places in the house. They, then, got a warrant to search the house and found the drugs they suspected. The Court considered the use of the imager as a search that violates the Fourth Amendment that requires a warrant for it to be reasonable even though the use of the imager does not physically trespass upon the defendant's home (Harper 2008). It created a zone of special protection within the private home that extends home expectation of privacy to other contexts as a minimum level of privacy.

According to Stephanie Stern (2011), protection of the home privacy led the American Supreme Court to extend the protection to rule in this case that conducting a thermal scan of the home from a public street without warrant is unconstitutional. The ruling is in consistence with the *Katz* as it did not rely on the premises-based test but on the expectation of privacy test as Kyllo seeks to buffer from others including law enforcement officials the interior of his home.

3.12 Aerial Imagery and Surveillance

Lastly, the capturing of aerial photographs or conducting aerial surveillance by law enforcement agencies for evidence collection in the criminal investigation is also in question with regard to its implications on the privacy of the accused. Aerial imagery or surveillance, also known as aerial search, can be done using fixed-wing aircrafts or helicopters (power 1989). In the past few years, unmanned aerial vehicles (UAVs) or unmanned aerial systems (UASs), commonly known as drones, were envisioned to be used for a number of purposes including search and rescue as well as fighting wildfires. They were also envisioned for the use in dangerous tactical police operations (Stanley & Crump 2011). This has raised privacy concerns if they are used for law enforcement activities in criminal investigation. Some argued that aerial images captured using these aircrafts, helicopters or drones invade one's privacy if the images are captured from a secluded backyard in which the person has a reasonable expectation of privacy from onlookers (Craig 2007).

Some American courts also evaluated the reasonableness of expectation of privacy from aerial surveillance in terms of the likelihood that such observations would occur (United States v DeBacker 1980). But, the Supreme Court excluded these situations from the search that requires warrant. It held in the the *California v Ciraolo* case that a warrant is not needed by law enforcement officials to take aerial photographs. It concluded that the naked

eye observations of a backyard at an altitude of 1000 feet do not constitute a search under the Fourth Amendment because the observations were made from public navigable airspace. The case involves aerial surveillance in California in which police suspected that marijuana was being grown in the backyard of a suburban home in which the surveillance using a fixed-wing aircraft observed the marijuana growing within the curtilage of the defendant's residence.

The Supreme Court also had the chance to uphold its position in the *Dow Chemical Co. v United States*. In this case, the police observed an industrial chemical plant as the corporate owner of this plant disallowed the Environmental Protection Agency (EPA) to inspect it. The EPA hired a commercial aerial photographer to fly over the plant and to take photographs of the open areas around the plant and between its buildings with a standard precision aerial mapping camera. The photographer captured the images using technological aids rather than naked-eye observations. The Court considered this activity as not infringing upon the reasonable expectation of privacy on the grounds that the photographs here are not so revealing of intimate details as to raise constitutional concerns and that the camera used in the aerial search was one that was publically and commonly available.

The Court further reached a similar conclusion in the *Florida v Riley* case, which involves helicopter surveillance. In this case, a police officer using a helicopter circled over an interior of the curtilage of a residence in Florida at an altitude of 400 feet based on information he received that marijuana was being grown in a greenhouse near the owner's mobile home. He spotted the marijuana through the openings in the roof. Although no warrant was issued, the court held that the search was constitutional. According to Brian Craig, the conclusions reached by the American Supreme Court in these cases were based on whether the technology used in capturing the images is in general use or not. In the cases that involve the use of thermal imaging the Court ruled that the use of thermal image is considered search that requires warrant as the device used is not in the use of the general public contrary to the use of aerial imagery devices that are not in the use of the general public (Craig 2007).

A similar conclusion is reached by Bleasdale (2014) as saying that the exact limits of the use of drones to conduct surveillance for law enforcement activities without warrant may be determined in the future by what becomes general public use. However, as drones are potentially powerful surveillance tools, Jay Stanley and Catherine Crump call for affording Fourth Amendment protection to individuals against law enforcement agencies' use of drones for the purposes of criminal investigation through imposing rules, limits and regulations on their use in order to preserve the reasonable expectation of privacy. Interestingly, the Association for Unmanned Vehicle Systems International (AUVSI) issued an Unmanned Aircraft System Operations Industry "Code of Conduct" in 2012 in which it promised to operate drones in a manner that respects the privacy of individuals (Cavoukian 2012).

4. Conclusion

Judging from the experiences of the advanced liberal democratic nations that tend to respect human rights such as the USA in which the situation has raised some problems and the need for a balancing test, this requires balancing the law enforcement interest in evidence collection with the privacy right in the criminal proceedings of Malaysia and Sudan. Meaning that the powers given to law enforcement agencies in the process of evidence collection in the two countries on the grounds of serving the law enforcement interest in evidence collection are in need of a revaluation that affirms the rights of the accused person, especially his or her privacy right.

Acknowledgement

The authors would like to record their appreciation to Universiti Kebangsaan Malaysia for providing research grant, No. GUP-2016-074.

References

Alzou'bi, S. et al. (2014). Artificial intelligence in law enforcement, a review. *International Journal of Artificial Intelligence & Applications (IJAIA), 4*(4), 5. https://doi.org/10.5121/ijait.2014.4401

Awade, M. M. (1988). Huquq al-Insan wa al-Ijra'at al-Man'eyah wa Ijra'at al-Taharri: Dirasah fi al-Qanun al-Sudani, *Second Conference of the Egyptian Section of A.I.D.P*: Protection of human rights in the criminal procedure of Egypt, France and the United States, Alexandria, Egypt, 108.

Bambauer, J. (n.d.). The lost nuance of big data policing. *Texas Law Review, 94*, 3.

Bedi, M. (2014). Social networks, government surveillance and the Fourth Amendment mosaic theory. *Boston University Law Review, 94*, 1819.

Bellia, P. L. (2004). Surveillance law through cyberlaw's lens. *The George Washington Law Review, 72*(6), 1379.

Bignami, F. (2015). The US legal system on data protection in the field of law enforcement: Safeguards, rights and remedies for EU citizens. *European Parliament, 17*. https://doi.org/10.2139/ssrn.2705618

Birrell, E. (2015). *Technology and the Fourth Amendment: balancing law enforcement with individual privacy, 14*. Retrieved January 28, 2016, from http://www.eecs.harvard.edu

Bleasdale, T. (2014). Privacy protections implicated by the domestic use of unmanned aerial vehicles or drones. *OLR Research Report, Connecticut General Assembly*, May 12. Retrieved June 18, 2016, from https://www.cga.ct.gov/2014/rpt/2014-R-0137.htm

Cavoukian, A. (2012). *Privacy and drones: unmanned aerial vehicles.* Retrieved June 19, 2016, from https://www.ipc.on.ca/images/Resources/pbd-drones.pdf

Craig, B. (2007). Online satellite and aerial images: issues and analysis. *North Dakota Law Review, 83*(1), 562.

Craig, J. D. R. (1997). Invasion of privacy and Charter values: the common-law tort awakens. 42 McGill LJ, 355.

Dilek, S. et al. (2015). Applications of artificial intelligence techniques to combating crimes: a review. *International Journal of Artificial Intelligence & Applications (IJAIA), 6*(1), 21. https://doi.org/10.5121/ijaia.2015.6102

Doyle, C. (2012). Privacy: an overview of the Electronic Communications Privacy Act, Congressional Research Service. Retrieved August 28, 2014, from www.crs.gov

Friess, N. (2012). When rummaging goes digital: Fourth Amendment particularity and stored e-mail surveillance. *Nebraska Law Review, 90*(4), 979.

Gihad, G. H. M. (1991). *Huqoq al-Insan fi Marhalat al-Muhakamah*. Cairo: Dar al-Nahdhah al-Arabiyyah.

Goldfoot, J. (2011). The physical computer and the Fourth Amendment. *Berkeley Journal of Criminal Law, 16*(1), 114.

Harper, J. (2008). Reforming Fourth Amendment privacy doctrine. *American University Law Review, 57*(5), 1381-1403.

Hassan, K. H. (2012). Data protection in employment: new legal challenges for Malaysia. *Computer Law and Security Review, 28*, 696-703. https://doi.org/10.1016/j.clsr.2012.07.006

Hassan, K. H., & Bagheri, P. (2016). Data Privacy in electronic commerce: Analysing legal provisions in Iran. *Journal of Internet Banking and Commerce, 21*(1), 1-14.

Hassan, K. H., Abdelhameed, A., & Ismail, N. (2018). Modern means of collecting evidence in criminal investigations: Implications on the privacy of accused persons in Malaysia. *International Journal of Asian Social Science, 8*(7), 332-345. https://doi.org/10.18488/journal.1.2018.87.332.345

Hong, L. (2011). The conflict and balance between government's information right and citizen's privacy right. *Journal of Politics and Law, 4*(2), 104.

Jesdanun, A. (2001). Privacy, security, censorship: upcoming net challenges. *The Malay Mail*, 1 January, 18.

Kerr, O. S. (n.d.). Search warrants in an era of digital evidence. *Mississippi Law Journal, 75*, 86.

Lederer, F. I. (1984). Scientific evidence: an introduction. *William and Mary Law Review, 25*(4), 518.

Levin, A., & Nicholson, M. J. (2005). Privacy law in the United States, EU and Canada: the allure of the middle ground. 2.2. UOLTJ, 357-395.

Madgwick, D., & Smythe, T. (1974). *Invasion of Privacy.* London: Pitman.

Majmudar, K. B. (1993). Daubert v. Merrell Dow: a flexibility approach to the admissibility of novel scientific evidence. *Harvard Journal of Law & Technology, 7*(1), 188.

McHarg, A. (1999). Reconciling human rights and the public interest: conceptual problems and doctrinal uncertainty in the jurisprudence of the European Court of Human Rights. *The Modern Law Review, 62*(5). https://doi.org/10.1111/1468-2230.00231

Murphy, E. (2013). The politics of privacy in the criminal justice system: information disclosure, the Fourth Amendment, and statutory law enforcement exemptions. *Michigan Law Review, 111*(4), 516.

Orofino, S. (1996). Daubert v. Merrell Dow Pharmaceuticals, Inc.: the battle over admissibility standards for scientific evidence in court. *Journal of Undergraduate Sciences, 3*, 111.

Overton, B. F., & Giddings, K. E. (n.d.). The right of privacy in Florida in the age of technology and the twenty-first century: a need for protection from private and commercial intrusion, 45.

Power, R. C. (1989). Technology and the Fourth Amendment: a proposed formulation for visual searches. *The Journal of Criminal Law & Criminology, 80*(1), 19. https://doi.org/10.2307/1143764

Reinert, A. A. (2010). Public interest (s) and Fourth Amendment enforcement. *University of Illinois Law Review, 5*, 1464.

Safavi, S., & Shukur, Z. (2014). Conceptual Privacy Framework for Health Information on Wearable Device. *PLoS ONE, 9*(12), e114306. https://doi.org/10.1371/journal.pone.0114306

Schmidt, L. A. (2012). Social networking and the Fourth Amendment: location tracking on Facebook, Twitter and Foursquare. *Cornell Journal of Law and Public Policy, 22*, 536.

Sklansky, D. A. (2015). Two more ways not to think about privacy and the Fourth Amendment, 82, 224.

Solove, D. J., & Schwartz, P. M. (2015). *An Overview of Privacy Law*. Portsmouth: IIPP Publication.

Stanley, J., & Crump, C. (2011). Protecting privacy from aerial surveillance: recommendations for government use of drone aircraft. *American Civil Liberties Union*, December. Retrieved June 17, 2016, from https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf

Thompson, S. (2006). Rights of the accused in criminal law. Yahoo Contributor Network, 23 October 2006. Retrieved May 22, 2013, from http://voices.yahoo.com/rights-accused-criminal-law-96584.html

Webber, D. (1984). Fourth Amendment--of warrants, electronic surveillance, expectations of privacy, and tainted fruits. *Journal of Criminal Law and Criminology, 75*(3), 630-652. https://doi.org/10.2307/1143636

Winn, P. (2008). *Katz* and the origins of the reasonable expectation of privacy test. *Mc George Law Review, 40*(1), 1-12.

Yaakob, H. (2016). Facing up to the legal challenges arising from the human variome project. *Malayan Law Journal, 4*, lxxxix.

Cases

Berger v New York, 388 U.S. 41 (1967).

California v Ciraolo, 476 U.S. 207, 214 (1986).

California v Greenwood, 486 U.S. 35 (1988).

Dow Chemical Co. v United States, 476 U.S. 227 (1986).

Daubert v Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Florida v Riley, 488 U.S. 445-52 (1989).

Katz v United States, 389 U.S. 347, 352 (1967).

Kyllo v United States, 533 U.S. 27, 31 (2001)

Olmstead v United States, 277 U. S. 438 (1928).

Goldman v United States, 316 U. S. 129 (1942).

People v Diaz, 244 P.3d *501, 509* (Cal. 2011).

Riley v California, 134 S. Ct. 2473 (2014).

Smith v Maryland, 442 U.S. 735 (1979).

State v Smith, 920 N.E.2d 949, *955* (Ohio 2009).

State v Wickline, 440 N. W. 2d. 249 (1989).

State v Buckman, 613 N. W. 2d. 463 (2000).

Terry v Ohio, 392 U. S. 1, 20-20 (1968).

United States v United States District Court, 407 U. S. 297, 313 (1972).

United States v New York Telephone Co., 434 U. S. 159, 169 (1977).

United States v Carey, 172 F.3d 1268 (10th Cir. 1999).

United States v King, 509 F. 3D (11th Cir. 2007).

United States v Miller, 425 U.S. 435, 443 (1976).

United States v Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

United States v Torres, 751 F.2d 875, 877 (7th Cir. 1984).

United States v Pinson, 24 F.3d 1056 (8th. Cir. 1994).

United States v Ford, 48 F.3d 1282, 1284 (D.C.Cir.1995).

United States v Allen, 675 F.2d 1373, 1381 (9th Cir. 1980)

United States v DeBacker, 493 F. Supp. 1078, 1081 (W.D. Mich. 1980).