Webology, Volume 4, Number 3, September, 2007

Cybercrime and the Law: An Islamic View

Mansoor Al-A'ali
Department of Computer Science, College of IT, University of Bahrain, P.O. Box 32038, Bahrain. Tel: +973-39607724 Email: mansoor.alaali (at) gmail.com, malaali (at) itc.uob.bh

Received February 22, 2007; Accepted September 20, 2007

Abstract

E-crime today presents one of the major challenges to law enforcement. Information technology is facing waves of laws guarding the interest of people using the Web technology. These laws were derived from the common laws and legislations applied in general crimes. With over one billion Muslims in this world, several calls were raised in the Islamic countries to establish a law suitable to handle computer crimes which matches the Islamic Shar'iah law. In this research, we have analyzed the 'Adellah' (الأدلة) (Shar'iah Evidences of Quran, Hadith and Imams sayings) to verify the outlook of Islam in computer crime. We propose an introductory computer crime law from an Islamic point of view which we believe will initiate further research in this important field.

Keywords

Computer Crime; Computer Crime Law; Texas Law; Islamic Law; Cybercrime

---

Introduction

Computer crime or e-crime presents one of the major challenges of the future to law enforcement (Backhouse & Dhillon, 1995; Dhillon & Moores, 2001; Dhillon et al., 2004; Ernst & Young, 2004). E-crime is part of or involved in all 'traditional crimes' such as drug trafficking, people smuggling and money laundering (DTI/PWC, 2004). What is really threatening is that younger people are involved in such crimes and that people in general would not hesitate to use the Internet to commit different types of crimes ranging from copying what is copyrighted to drug smuggling and pornography. Further, computer crime is of a global nature and this makes dealing with it particularly challenging. The challenges for computer crime investigators have been summarized by Barbara Etter (2001) as follows:

1. *Anonymity*
2. *Global reach (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimisation)*
3. *The speed at which crimes can be committed*
4. *The potential for deliberate exploitation of sovereignty issues and cross-jurisdictional differences by criminals and organised crime*

5. *The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints or DNA; and The high costs of investigations.*

The management of e-crime poses numerous and diverse challenges and include (*Australian Police Commissioners' Conference Electronic Crime Working Party* 2000, pp. 25-28; Rees 2000, pp.16-19):

1. *Bridging multijurisdictional boundaries.*
2. *Retaining and preserving evidence.*
3. *Acquiring appropriate powers.*
4. *Decoding encryption.*
5. *Proving identity.*
6. *Knowing where to look for evidence.*
7. *Tackling the tools of crime and developing tools to counter crime.*
8. *Rethinking the costs and priorities of investigation.*
9. *Responding to crime in real time.*
10. *Coordinating investigative activities.*
11. *Improving training at all levels of the organisation.*
12. *Developing strategic partnerships and alliances.*
13. *Improving the reporting of electronic crime.*
14. *Enhancing the exchange of information and intelligence.*
15. *Acquiring, developing and retaining specialist staff. and*
16. *Avoiding 'tech-lag' (or ensuring access to cutting edge technology).*

The US Electronic Frontier report (PWGUCI, 2000) states that 'balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead'. The UK has also demonstrated its concern relating to anonymity and a range of other issues through the creation of the Regulatory and Investigatory Powers Act. The FBI's Carnivore system has also been the subject of much criticism and debate.

Most of the currently accepted western basic principles of ethics in research are consistent with the instructions of Islam (Editorial, 2006). Prophet Mohamed (peace be upon him) said, I was sent to complete the epitomes of Ethics (Abdel-Baky, 1951). The teaching of Islam covers all the fields of human activity. The instructions, which cover everyday activity is called *Shar'iah*. Western countries do not understand why Muslims are against implementation of secularization in their countries. We have to understand that Islam is not only a religion; it is a way of life. As mentioned earlier, the *Shar'iah* controls every day activities of Muslims (Editorial, 2006).

Research about computer crime is not isolated from research about computer ethics. The potential of writing on computer ethics and related subjects to contribute to a deeper understanding of inequalities surrounding the use of information and communication technologies is threatened by forms of technological determinism and liberalism (Alison, 2001). Computer crimes can take many forms, from cyber stalking to child pornography (Newman & Clarke, 2003). Cyber stalking describes stalking behavior executed by means of some aspect of information and communication technologies. The ever increasing use of the Internet by 'criminals' has prompted a rush of legislation and other interest (Reno, 1999). Unfortunately, despite a number of high-profile cases reported both in print media and on the Internet, the topic has yet to receive systematic analysis against an appropriate theoretical framework (Alison, 2001). Such a theoretical framework must include a combination of an understanding of the psychological phenomenon of stalking, an understanding of Internet crime.

Some people may argue that our rights of privacy are "socially constructed," meaning that they change over time under the influence of many human forces and institutions, including technology, culture, and law (Levine, 2003). Another factor that affects our rights is the strength of the arguments that we use to think about them. Levine (2003) presents the following ten factors relating to privacy which we feel serve our argument for presenting a discussion about computer crime from an Islamic point of view (Yousif, 2002), these factors are:

1. *Freedom: Being able to conceal our behavior from others protects us from punishment, discrimination at work, social ostracism, and unpleasant criticism.*
2. *Property rights: Perhaps information about me belongs to me, just as anyone's body is his or her property.*
3. *Informed consent: As a general matter, we should not do things to others without their permission.*
4. *Personality development: Perhaps we need opportunities for private reflection and experimentation if we are to develop complex personalities.*
5. *Avoidance of discrimination: Powerful people sometimes want to act on the basis of morally irrelevant information.*
6. *Avoidance of defamation: It can be harmful for people to accuse their fellow citizens of misconduct, especially when their accusations are either false or unsubstantiated.*
7. *Happiness: Although there are other moral values besides happiness (consider justice, fairness, compassion, and freedom), we generally think that it is right to make people as happy as possible, at least all else being equal.*
8. *Equality of power: Knowing information about people is a source of power. Protecting the rights of ordinary people to withhold information strengthens them against governments and large firms.*
9. *Separation of zones: Many people believe that it is important to keep society carefully divided into zones such as that of the market, the family, the military, religion, politics, scholarship, and social relationships.*
10. *Rights of association: We have both legal and moral rights to associate in voluntary groups.*

As the United Nations (UN) points out (1999, p.48): Today, it is technologically possible for an operator to punch a keyboard in country A so as to modify data stored in country B, even [though] the operator does not know that the data are stored there, to have the modified data transferred over a telecommunication network through several other countries, and to cause an outcome in country C. On the basis of the physical act, three or perhaps more countries will have been involved and may have a claim to jurisdictional competency.

Testing Muslim audience computer crime standing

In order to evaluate the level of knowledge and awareness about computer crime in a typical Muslim country, we prepared a simple but carefully prepared questionnaire and identified three groups for the evaluation process. The three groups chosen are shown in Table 1 and consist of 1) ordinary parents of average education and Internet knowledge, 2) final year university students who have been using the Internet for a wide variety of uses, 3) school social guidance staff who look after the teenagers problems at schools. These three groups were carefully chosen as a real representative of the society of Bahrain and who will give genuine answers to our survey such that the results of this survey can be used as an indicator of the awareness of computer crime in our society. No emphasis was placed on the male/female issue and the participants were of mixed sexes.

We carried out this simple survey in order to get an indication if it is worth considering this line of research which will result in proposing an introductory computer crime law from an Islamic point of view. It is clear that this direction of research is well worth pursuing.

Table 1: Groups of participants in the computer crime law evaluation

Group	Total Number
Group 1: Ordinary Parents	25
Group 2: Final year university students	31
Group 3: School social guidance staff	14

The questionnaire consisted of the following questions and the results are shown in the corresponding tables.

1. Do you think that the Internet use in general should be governed by a specially prepared law in order to protect society although this means loss of privacy?

Table 2: Should the Internet be governed by a specially prepared law in order to protect society

Group	Total Number	Yes	No
Group 1: Ordinary Parents	25	21	4
Group 2: Final year university students	31	19	12
Group 3: School social guidance staff	14	12	2

The results shown in Table 2 are very interesting since the participant has to choose between possible loss of privacy and the need to protect society. The overwhelming majority of groups support an Internet law and we believe this is triggered by parenthood protection. The fact that 4 out of 25 (16%) of parents are against such law is an indication that loss of privacy is seen as negative deliverable of this law.

2. Should the new law be based on Islamic teachings as per the Quran and the Hadiths?

Table 3: Should the new law be based on Islamic teachings as per the Quran and the Hadiths?

Group	Total Number	Yes	No
Group 1: Ordinary Parents	25	18	7
Group 2: Final year university students	31	26	5
Group 3: School social guidance staff	14	12	2

The results in Table 3 indicate that Muslims believe that most if not all legislations should be based on Quran and the Prophet's Hadiths. It is believed that Muslims feel safer this way and they know the boundaries of the law, otherwise such law will be driven by a group of individuals, e.g., parliament, who at a given period of time and based on certain individual understandings will produce such a law which might later be found to have a number of shortcomings. The number of participants who opted for a 'no' answer from the three groups is still significant. This could be interpreted in many different ways and we will not delve into such explanations because we feel that they are outside the scope of our research.

It is noticed that group 2 have less reservations about the law being based on Islamic teachings than having a law in general as can be seen in Tables 2 and 3. This must mean that they feel safer with a law being based on Islam which does not allow organizations to implement their own style of monitoring and governance. In the case of group 3, there is

no difference to them, the majority of them, 12 out of 14, are in support of a law regardless. Group 3 are involved with students' social problems which have been on the increase and are affecting schools teenagers and appreciate a law to protect society in general and the teenage students themselves.

Computer Crime and Islam

Shar'iah has a very high level of proof for the most serious crimes and punishments. If proof is not as specified then the crime must be considered a lesser crime. The major myth is that judges in Islamic nations have fixed punishments for all crimes. The judge under *Shar'iah* is not bound by precedents, rules, or prior decisions as in English common law. Hadd crimes, the most serious crimes in *Shar'iah* law, are murder, apostasy, making war upon Allah and His messengers, theft, adultery, defamation, false accusation of adultery or fornication, robbery and consumption of intoxicants. These are considered crimes against Allah. *Tazir* crimes are acts which are punished because the offender disobeys Allah's law and word. Tazir crimes are crimes against society. A *Qesas* crime is one of retaliation. If you commit a Qesas crime, the victim has a right to seek retribution and retaliation. The concept of retribution was found in the first statutory "Code of Hammurabi" and in the law of Moses in the form of "an eye for an eye." Muslims add to that saying "but it is better to forgive."

Contemporary common law today still is filled with the assumptions of retribution. The American justice system has adopted a retribution model which sets fixed punishments for each crime. The American federal code contains "mandatory minimum" sentences for drug dealing. Many states have fixed punishment for drug, violence and the use of particular weapons. Qesas crime is simple retribution: if one commits a crime he knows what the punishment will be.

Diya has its roots in Islamic law and dates to the time of the Prophet Mohammad when there were many local families, tribes and clans. The Prophet was able to convince several tribes to take a monetary payment in retribution for damage to the clan or tribe. Diya is paid by the offender to the victim if he is alive. If the victim is dead, the money is paid to the victim's family or to the victim's clan or tribe. The assumption is that victims will be compensated for their loss. Under English common law, the victim or family must sue the offender in a civil tort action for damages. *Qesas* law combines the process of criminal and civil hearings into one, just as the "civil law" is applied in many nations on Earth. Qesas crimes are compensated as restitution under common law and civil law. The Qesas crimes require compensation for each crime committed.

With the spectacular growth of high-technology industry, computers and communication have become the backbone of our new life style. Consequently, computers have created a host of potentially new misuses, and the computer-related crime has become a growing phenomenon that involves traditional criminal activities such as theft, fraud, forgery and mischief (Audit Commission, 1998). In spite of the difficulties to determine when the first crime involving a computer actually occurred, in early 1974, David Stryker, John Shore and Stanley Wilson of the United States Naval Research Laboratory subverted operating system of a Univac 1108 computer using security violating Trojan horse techniques to obtain unauthorized and surreptitious access to classified information. The US government figures show that money made by criminals through cybercrime now exceeds that from drugs and narcotics. Some reports claim that the cybercrime market is worth up to $1.6tr a year (Little, 2006).

Computer security represents a growing concern for societies and organizations. Previous studies have addressed the computer crime threat (ISO BS17799, 2005), Willison, 2006; Willison & Backhouse, 2006). However, there has been a lack of focus given to the

relationship between the human behavior of offenders during the perpetration of computer crime and other relevant issues such as social and religious upbringing and behavior. Yet insights into this relationship could feasibly be used to address such dangerous risks. The goal would be to understand the offender behavior and look into other ways of bringing to the attention of the individual's benefits and punishments which are not necessarily related to man made to the criminal law. Hence the computer security strategy should aim to support the criminal act through the implementation of safeguards which influence the offender's inclinations and wider fears (Al-A'ali, 2006).

Organizations can currently draw on a number of means for computer crime guidance. These include the use of risk assessment techniques (Peltier, 2004), international standards, such as ISO BS17799 (2005), or the 'baseline security' approach (Parker, 1998) and (Willison, 2006), where controls are selected based on best practice principles. However, the major question will always remain, is it enough to have standards and crime laws to prevent or reduce crime? Clearly unless we address the human behavior itself and appeal to the individual with other forces of control which should on the whole be self imposed, we shall continue to have computer crime.

We can define computer crime generally as a crime accomplished through special knowledge of computer technology. The law has been too slow to understand and react to the rapid changes in technology. We have recently witnessed that previous laws are unable to handle these crimes. The first comprehensive proposal for computer crime legislation was a federal Bill introduced in the US Congress by Senator Ribikoff in 1977 (Schjolberg, 2003). The Bill was not adopted, but this pioneer proposal created awareness all around the world.

A number of western nations have long started their assessments of existing laws for their suitability or adaptability to computer crimes. The legislature of Texas - as an example - passed the computer crime law in 1985. A great number of specialists in different law fields, information technology, politics and economics have participated to prepare this law and it has been modified several times during a short time. This law shows the efforts spent to achieve the law to win the battle of this growing threat.

The question is: Do these laws work actively and do they provide the right punishment to fit the crime? The evidences show that the risk of a computer crime remains high, and that despite deploying an enviable range of security technologies and new laws, people and organizations still fall victim to attacks that resulted in significant financial loss (CSI/FBI Survey, 2003). The Australian survey also shows that the total losses for 2003 are more than double quantified losses in 2002 (Australian Survey, 2003).

One out of every four persons on the planet is a Muslim (Hassan, 1990) and for those who believe in perfecting justice through the Islamic law, it is very important to develop the Islamic outlook to computer crime especially since we know that most Islamic countries place it at the center of their legal codes like Saudi Arabia, Sudan and Iran (Crystal, 2001; Kamali, 1994). Facts decide the importance of the Islamic law to minimize computer crimes, by providing a worldly punishment as well as that in the hereafter (Afifi, 2003). Researchers proved that computer crimes with high technology like money theft, information theft, or betrayal are not new. Computer crimes need a new Islamic theory (Alfaifi, 2001).

The questions are: What is the basis of the Islamic law for computer crime? When and where the Islamic law was established? How would the Islamic law that was established in the seventh century handle the new technology issues and provide a suitable law for computer crimes? How would the Islamic law compare with the western laws like Texas Computer Crime Law? This research attempts to answer these questions in order to

establish an introduction of the Islamic computer crime law, and to prove that an Islamic computer crime law can contribute to the well being of humanity in parallel with the western law.

We have surveyed the literature and did not find much work published about Islamic law and the information technology with the exception of (Norazlina et al., 2003) and (Mancuso, 2007). Both of these research paper focus on e-commerce crimes and Islam.

Before we start to propose a new Islamic computer crime law, we must describe the basic principles of the Islamic law in general. We will then compare the new Islamic computer crime law with the Texas Computer Crime Law. Then we will survey the Quranic verses and Prophet Mohammad sayings to find and analyze the Islamic evidences that can be related to computer crimes in Texas Computer Crime Law. Our final objective is to propose the Islamic computer crime law.

Islamic law originated with the birth of Islam in the seventh century with the coming of Prophet Mohammad (Pbuhwa), as a common law. Islamic law is known as *Shar'iah* law, and Shar'iah means the path to follow God's Law. Shar'iah law is holistic or eclectic in its approach to guide the individuals in most daily matters. Shar'iah law controls, rules and regulates all public and private behavior (Wiechman *et al.*, 1994). The theoretical assumption of the Islamic Law is to protect the five important indispensables in Islam: Religion, Life, Intellect, Offspring and Property. Islamic Law has provided a worldly punishment in addition to that in the hereafter (Madkoar, 1980). Islam has, in fact, adopted two courses for the preservation of these five indispensables:

1. Through cultivating religious consciousness in the human soul and the awakening of human awareness through moral education.
2. By inflicting deterrent punishment, which is the basis of the Islamic criminal system. Therefore, the limits or "*Hudud*," and retaliation (*Qisas*) and Discretionary (*T'azir*) punishments have been prescribed according to the type of the crime committed.

In this research, we address the major issues of human behavior in relation to Islamic religion and computer crime. This research presents a new computer crime law based on Islam. To our knowledge, there is no Islamic Computer Crime law till now and hence our proposed new Islamic Computer Crime law is the first. We evaluate the leading computer crime law which is the Texas Computer Crime law in relation to our newly proposed Islamic Computer Crime law. The Texas Computer Crime Law and other existing similar laws are conclusive and pioneering by all accounts, but, it is our belief that they actually do not trigger the emotions of Muslims and hence can only be applied in the court of law. It is our belief that once a crime is in the court of law then the damage had been done and the court will keep busy with a constant stream of a wide variety of cases if they are discovered. If we appeal to the Muslim before he/she commits the crime and put the issue of computer crime in perspective, then we are more likely to succeed in stopping crime.

Computer Crime Law

There are a number of computer crime laws developed by many western countries, for example Texas Computer Crime Law. Section 33.02 in Texas Computer Crime Law defines the breach of computer security in four points (Texas Computer Crime Law, 1994):

1. *A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.*
2. *A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system*

to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.

3. *An offense under this section is a Class A misdemeanor unless the actor's intent is to obtain a benefit or defraud or harm another, in which event the offense is:*
    - *a state jail felony if the value of the benefit or the amount of the loss or harm is less than $20,000; or*
    - *a felony of the third degree if the value of the benefit or the amount of the loss or harm is $20,000 or more.*
4. *A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.*

In Islam, the basis of law is the Quran (Islam Holy Book) and Hadith (Prophet sayings). In this section, we have collected and presented the Adellah (Shar'iah Evidences) of Quran and Hadith which relate to the three points of the breach of the computer security in relation to the Texas Computer Crime Law. We use the Quran translation by F. Malik. In this section we have simply collected a few of the Quranic versis and a few of the Prophet sayings in preparation for the next sections.

This section dedicates the importance of privacy. The computer hardware or software is a property of someone. Access would be unauthorized if an offender:

1. Is not himself entitled to control access of the kind in question to the program or data.
2. Does not have consent to access the program or data from a person who is so entitled.

Table 4 shows the Adellah for: "*A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner*."

Table 4. Adellah for A person commits an offense

Adellah	Explanation
ALLAH (God) said: "O believers! Do not enter houses other than your own until you have sought permission and greeted their inmates " (Ayah, An-nur, 27).	In this Ayah, Allah decides: If you wanted to enter a houses other than your own ask the owners permission beforehand. So from the Islamic principles you cannot access the properties others without their permission, this is the Islamic approach to the rights of privacy.
ALLAH said: "O believers! Avoid immoderate suspicion, for in some cases suspicion is a sin, Do not spy on one another" (Al-Hujurat, 12).	In this Ayah, ALLAH command: Do not spy on one another. Therefore, from the Islamic principles you cannot spy on the secrets of others including those hidden or stored inside computers despite your suspicion.
Prophet Mohammad (peace be upon him) said: "It is better for a Muslim to mind his own business" (Al-Muatta, 1980).	In this Hadith, the Prophet tells us that we are good Muslims if we leave other peoples' business alone. Therefore, from the Islamic principles you cannot allow your curiosity on other peoples' business to delve in their property including the information in their computers.
Prophet Mohammad (peace be upon him) said: "Permission is for having a look" (Al-Bukhari, 1987).	In this Hadith, the Prophet tells us that the main aim of permission is for having a look. Therefore, from the Islamic principles you cannot have a look inside other persons' properties if they did not allow you, and the computer is a property.

Table 5 presents the Adellah for: 3.2 "*A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict access to a computer, computer network, computer system, or data.*" This section dedicates the importance of trust. The computer system password, identifying code, personal identification number, debit card number, bank account number, or information that may be given on trust. To gives any confidential information to another person without effective permission is a betrayal of trust.

Islamic Computer Crime Law Proposal

In this section, we have put together a proposal for an Islamic computer crime law which we hope will initiate further future research by computer security specialists, law makers and theologians alike. It is an arguable discussion whether to call this a computer crime law or a computer crime ethics law; it is our belief that the latter applies more since the aim is to work on the human being to stop him or her from committing the crime rather than handing out the punishment. There is no disagreement that punishment can be a deterrent but prisons are never and will never be empty. Our proposed computer crime law is more of prevention rather than a cure for many in society in general rather than a deterrent to an isolated individual.

1. Privacy

"*A person should have permission before having a look*". It is prohibited for any person to come (physically or logicality) near computers or their accessories for curiosity or to look at their contents without a prior permission of the owner and he should be aware of the limit of the given permission.

2. Trust

"*A person should be trust worthy even with a betrayer*". Any person who receives some confidential information or a password to access a computer should not give them deliberately to any person without a prior permission from the owner. Muslims and non-Moslems are equal to be trust worthy. It is interesting here that this item states that one cannot betray someone else who had betrayed them beforehand. Further, this item states that Muslims and non-Muslims are equal in trust worthiness.

3. Theft

"*It is prohibited to get other persons properties illegally*". It is not permitted to get benefits of the contents of a computer or through it without permission. Any action like this is considered a theft.

4. Promise

"*Muslims should respect their terms*". This condition states that it is prohibited to use other persons computers or get what is recorded on them of worthy programs or information without a prior permission. Muslims and non-Moslems are equal at that condition.

Table 5. Adellah for Privacy, Trust, Theft and Promise

ALLAH said: "Allah commands you to give back the trusts to their rightful owners" (An-nessa, 58).
ALLAH said: "O believers! Do not betray the trust of Allah and His Prophet, nor

violate your trusts knowingly" (Al-Anfal, 27).
Prophet Mohammad (peace be upon him) said: "The signs of a hypocrite are three: Whenever he speaks, he tells a lie. Whenever he promises, he always breaks his promise. If you trust him, he proves to be dishonest. If you keep something as a trust with him, he will not return it." (Al-Bukhari, 1987).
Prophet Mohammad (peace be upon him) said: "Give back what you have been trusted with and do not betray those who have betrayed you". (Al-Hakeem, 1990)
ALLAH said: "O believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent." (An-nessa, 24)
ALLAH said: "Male or female, whoever is guilty of theft, cut off their hand (that was used in theft) of either of them as a punishment for their crime. This is exemplary punishment ordained by Allah." (Al-Maaeda, 38)
Prophet Mohammad (peace be upon him) said: "It's prohibited to take the Muslim wealth without his complete permission." (Al-Baihaqi, 1994)

Conclusion

The Internet has presented a new challenge to humanity in facilitating crimes which have no boundaries and may be no evidence or trace. Muslims tend to relate to and adhere to Islamic teachings which instill the fear of God and hence the main conclusion of this research is to argue the case for an Islamic computer crime law. We argued the case for a proposed computer crime law based on Islam which addresses the individual before the crime is committed and hence is more of prevention than a cure. The paper presented the proposed law. A survey arguing for the Islamic computer crime law was carried out which proves the need for such a law. We believe that this paper will instigate further research into the topic.

References

- Abdel-Baky, M.F. (1951). Al-Mowatae of Imam El-Aema wa Alem El Madina, Malek Ibn Anas, El-Shaeb Book. *Husn El Kholok*, Hadith # 8, p. 564.
- Afifi, K. (2003). *Computer Crimes and the Author Copyright*. Alhalabi Publishing, Lebanon, (In Arabic).
- Al-Baihaqi, Ahmad Bin Al-Husain (1994). *Al-Sunan Al-Kubra*, (In Arabic).
- Al-A'ali, M. (2006). Islamic Computer Ethics via the ACM Computer Ethics, *International Arab Conference on Information Technology* (ACIT'2006), Yarmouk University, Jordan, 19-21.
- Al-Bukhari, Mohammad I., Al-Bukhari, Sahih, Ibn Kather Publishing, 1987. (In Arabic).
- Al-Muatta, Malik Bin Anas (1980). Dar Ihiaa Altorath Publishing. (In Arabic)
- Alfaifi, M.A. (2001). *The Economic Crimes Adjudgments in the Computer*.
- Al-Hakeem, Mohammad Bin Abdullah (1990). Almustadrak, Dar Alkutob Publish, 1990. (In Arabic)
- Alison, A. (2001). Computer ethics in a different voice. *Information and Organization*, 11, 235-261.
- Audit Commission (1998). *Ghost in the machine: An analysis of IT Fraud and abuse*. London: Audit Commission Publications.
- Australian Survey (2006). Australian Computer Crime and Security Survey. Retrieved September 15, 2007, from http://www.auscert.org.au/render.html
- Backhouse, J., & Dhillon, G. (1995). Managing computer crime: A research outlook. *Computers and Security*, 14(7), 645-651.
- Crystal, Jill (2001). Criminal justice in the Middle East. *Journal of Criminal Justice*, Vol. 29.

- CSI/FBI. (2003). *CSI/FBI Computer Crime and Security survey* (2003). Computer Security Institute (CFI), San Francisco Federal Bureau of Investigation's Computer Intrusion (FBI). Retrieved September 15, 2007, from http://www.gocsi.com
- Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers and Security*, 20(8), 715-723.
- Dhillon, G., Silva, L., & Backhouse, J. (2004). Computer crime at CEFORMA: A case study. *International Journal of Information Management*, 24(6), 551-561.
- DTI/PWC (2004). *Information security breaches survey*. London: PWC.
- Editorial, Biomedical research ethics: An Islamic view, part I. *International Journal of Surgery* (2006).
- Ernst & Young (2004). *Global information security survey*.
- Etter, B. (2001). Computer crime. *The 4th National Outlook Symposium on Crime in Australia*. New Crimes or New Responses convened by the Australian Institute of Criminology and held in Canberra 21-22 June, 2001.
- Hassan, R. (1990). *Muslims in America: A Living Presence, Horizons*.
- The Holy Quran.
- ISO BS17799. (2005). *Information technology - security techniques - codes of practice for information security management*. Switzerland: International Organization for Standardization.
- Kamali, M. H. (1994). *Freedom of Expression in Islam*. First ed., Berita Publishing Sdn Bhd, Kuala Lumpur.
- Levine, P. (2003). Information technology and the social construction of information privacy: Comment. *Journal of Accounting and Public Policy*, 22, 281-285.
- Little, B. (2006). Protect and survive - against cyber crime Source. *Training Technology & Human Resources*, 19(4), 11-12.
- Madkoar, M.S. (1980). *The Effect of Islamic Legislation on Crime Prevention in Saudi Arabia*. Ministry of Interior, Kingdom of Saudi Arabia, (In Arabic).
- Mancuso, S. (2007). Consumer Protection in E-commerce Transactions: a First Comparison between European Law and Islamic Law. *Journal of International Commercial Law and Technology*, 2 (1).
- Newman, G., & Clarke, R. (2003). Superhighway robbery: Preventing e-commerce crime. Portland, Oregan: Willan.
- Norazlina, Zainul, Fauziah Osman, Siti Hartini Mazlan (2004). E-commerce from an Islamic Perspective. Electronic Research and Applications Journal, 3, 280-293.
- Parker, D. (1998). *Fighting computer crime: A new framework for protecting information*. New York: Wiley Computer Publishing.
- Peltier, T. (2004). Risk analysis and risk management. *Information Systems Security*, 13(4), 44-56.
- Reno, J. (1999). Cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President. Retrieved September 15, 2007, from http://www.usdoj.gov/ag/cyberstalkingreport.html
- Schjølberg, S. (2003). The Legal Frame Work - Penal Legislation in 44 Countries. Retrieved September 15, 2007, from http://www.mosstingrett.no
- Texas Computer Crime Law (1994). Retrieved September 15, 2007, from http://suefaw.home.texas.net
- United Nations (UN) (1999). *International review of criminal policy - United Nations manual on the prevention and control of computer-related crime*. UN, New York. Retrieved September 15, 2007, from http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html
- Wiechman, D.J., Kendall, J.D., & Azarian, M.K. (1994). *Islamic Law Myths and Realities*. University of Illinois.
- Willison, R. (2002). Opportunities for computer abuse: assessing a crime specific approach in the case of Barings.

- Willison, R. (2006). Understanding the offender/context dynamic for computer crimes. *Information, Technology and People*, 19(2), 170-186.
- Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, 16, 304-324.
- Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems*, 15(4), 403-414.
- Yousif, A.F. (2002). Information Technology in 21st Century: An Islamic Perspective.

Bibliographic information of this paper for citing:

Al-A'ali, Mansoor (2007). "Cybercrime and the Law: An Islamic View." *Webology*, **4**(3), Article 46. Available at: http://www.webology.org/2007/v4n3/a46.html

---
