History of legislation dealing with cyber crime literature review

Technology, Internet

Arguably, as computer technology develops, so does the criminal offences that come as a result of using computers and internet. The 21st century marks the peak season of various cyber crimes and cyber terrorism. As a matter of fact, human beings should learn and adopt to live with criminal activities associated with technology. Therefore, as a result of accepting reality, utilization of computer networks as well as development of cyberspace society, various strategies have been developed to perpetrate these crimes. The history of legislation to deal with cyber crimes began in 1970s. Generally, since the existence of computer technology, various crimes related to technology poses a big challenge to the law enforcing body, as well as legislation of laws. Known in the world as cyber crimes, these criminal offenses need additional and introduction of laws to help in investigations. In fact, most of the legislation took place in the early 21st century. As technology advances, cyber crimes also become complex, and so should be the legislation (Shahidullah, 2008).

Certainly, traditional penal laws helped in setting the pace on cyber crime legislations. But the critical problem is that the laws were written without having in mind the ever growing cyberspace. The complexity of legislations comes in terms of applicability, as well as the extend of its effectiveness in solving cyber crimes. Traditional legislation bases its decisions in describing various unethical behaviors that the community has qualified it as criminal wrongdoing. Since mid-90s, the realities of cyberspace began at an extraordinarily high pace, making the legislations unable to cope with the pace (Brenner, 2007).

Wall (2007) asserts that, cyber terrorism is common in a popular cultural context, but exceedingly complex to understand. In fact, to some extent its definitions are controversial. In order to develop legislation to control the cyberspace, many scholars had to identify various forms of these crimes, which may spawns every day. It includes fraud, scams, development of malicious codes, hacking, identity theft, child pornography, copyright violation, as well as cyber-stalking.

In United States, the first legislation that deals with cyberspace crimes is referred to as wire fraud statue. The statue forbids the use of wires of communication that are mostly utilized in international or interstate commerce as a strategy to consign fraud. The legislation of fraud statue took place long ago, but it still incriminates various computer crimes today. According to Brenner, the law needs a proof that demonstrates an arrangement to defraud either property of money. In the history of cyber space legislation, the ultimate goal of laws is to prevent crime as well as punish the offenders. Certainly, a potential perpetrator in the cyber space should be warned, which prevents him/her from committing crime. Cyberspace is an avenue of most of the crime, either by providing a suitable environment or being part of the cause (Brenner, 2007).

Conversably, history of legislation that deals with cyber crime has undergone many processes. Several individuals in the globe have become part of legislation process. The father and founder of skills and knowledge of investigating computer crimes is known as Donn Parker from USA. From early 1770s, Parker was involved in various researches on computer security and crime. He was a SCSC (Senior Computer Security Consultant) at SRI international. During this era Parker became the author of the 1st feral manual concerned with law enforcement on cyber crimes (Ching, 2010). Other individuals in USA who helped in implementing legislations and carrying out research on cyber crimes were Jay Bloombecker and August Bequai. After various legislations in USA, Norway in 1976 joined the force I fighting cyberspace crimes. It later spread to Germany, Netherlands, as well as Australia (Easttom, 2010).

Cyber crimes became an international issue, triggering the involvement of United Nation in 1983. The pioneering of security against cyber crimes led to the formation of Council of Europe. Internationally, CECCAEC (Council of Europe Conference on Criminological Aspects of Economic Crime) became the first in tackling computer crimes. The conference took place in 1976 in Strasbourg (Shahidullah, 2008). During the conference, various categories and types of computer crimes were established. The conference was beneficial as it laid down the foundation of various legislations on cyber crime, based on the type.

After the Council of Europe Conference, the Ribikoff bill followed. In 1977, the 1st comprehensive and significant scheme on computer crimes took place. United States Government Operations Committee was in the front in introducing the initiative. The staff discussed on many problems associated to computer crime, and introduced legislation that prohibited the use of unauthorized computers. In late 1977, senator Ribicoff came up with the Ribicoff bill. The bill prohibited the use of computers in various places. The bill later was introduced as Federal Computer Protection Act of 1977, which is valid up to date. In the real sense, the bill in question was not adopted, but it developed awareness in the globe on the impacts of using unauthorized computer (Easttom, 2010).

Thereafter, the Interpol became the first in addressing computer penal legislation and crime in an international arena. Perhaps, the Interpol members came up with a project and discussion in which Geneva Assemble approved in 1980/81. Questionnaires were circulated to all Interpol member states; basically, the questionnaire was on computer crimes. The findings asserted that the penal legislations were unsatisfactory (Brenner, 2007). Hence, it recommended on legislation in various fields which include erasure and modification of data, and unauthorized data disclosure. The summary and recommendations became the basis of harmonization of various penal codes in dealing with global cybercrimes.

In the year 1986, the OECD recommendations followed. The elected group of specialized in Paris discuses crimes related to the computer, as well as the call for changes on the penal codes. The committee listed various acts that constituted to computer crime. It included damage of data, computer forgery, unauthorized infringement as well as computer fraud. The acts guided in the legislation process (Ching, 2010). In the year 1989, the Council of Europe came up with another recommendation on various legal issues that surrounded computer crimes. The recommendations included a minimum list of computer sabotage, computer fraud, damage of programs and data, computer forgery, unauthorized production, unauthorized interception, and unauthorized access.

In 1995, council of Europe recommended on concerns on problematic procedural law related with information technology. The 1995 recommendation introduced eighteen principles that were categorized into seven chapters. The G-8 States came up with a team of experts to help in investigating high-tech crimes. Their main objective was to ensure that no crime went unnoticed in the world (Shahidullah, 2008). Another step towards the legislation to deal with cyber crimes came from the Stanford University, California, and Hoover Institution; it was called The Stanford Draft Convention of 200. Conference was aimed at the recommendation on legislation that will combat cyber terrorism and crime. Early in the 21st century, the Electronic frontier recommended approaches for addressing various unlawful behaviors on the internet.

The legislation that helps in combating cyber terrorism and crime has undergone a lot of changes, and additions. In the world today, the legislations are particularly relevant as it prevents many types of crime. In 2003, it was found that many children were exploited through internet. Hence, the protect act was passed; its intent was to provide security to children (Easttom, 2010). Invention and innovations take place in the technology world on a daily basis; therefore, new legislation should take place so as to counter on new cyber crimes. Generally, internet is a boon to education, business, science, and on a negative note crime. Cyber crimes affect human day to day activities, for example, it affects individuals and organization in a different capacity (Ching, 2010).

Undeniably, prevention of cyber crimes is better than curing it. Hence, individuals should be very cautious when using the internet, and being part of the cyber world. Online security should include protection, precautions, prevention, perseverance and preservation. Legislation and recommendations from various organizations and individuals are historically significant in achieving cyber security (Brenner, 2007). The legislation has given individuals the right to be protected by the law. But despite the presence of law, individuals should be careful when using internet. Lack of legislation to deal with cyber crimes will make the world the most insecure place to be. Internet has become part of human beings today, in that anything that comes from the internet is highly influential and effective, regardless of its outcome.

References

Brenner, S. (2007). Law in an Era of Smart Technology. Oxford: Oxford University Press.

Ching, J. (2010). Cyberterrorism. New York: Rosen.

Easttom, C. (2010). Computer Crime Investigation and the Law. New York. Springer.

Shahidullah, S. (2008). Crime Policy in America: Laws, Institutions, and Programs. New Jersey:

Wadsworth.

Wall, D. (2007). Cybercrime: The Transition of Crime in Information Age. London: Wiley.