ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COMMERCIAL TRANSCTIONS: A COMPARATIVE STUDY IN SHARĪ'H AND LAW

Thesis submitted for the partial fulfilment of the requirement for the degree of Ph.D in Sharī'ah (Islamic law and Jurisprudence)

Submitted by

Hafsa Abbasi

Reg. No. 23-FSL/PhDIJ/F11

Supervised by:

Dr. Hafiz Anwar

Professor of Sharī'ah

Co-Supervisor

Dr. Asim Iqbal

Assistant Professor of Law

DEPARTMENT OF SHARĪ'AH

FACULTY SHARĪ'AH AND LAW

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD

2018

PHD
341.754
HAA

Accession No. TH23764

Commercial Law
International Law

DEDICATION

This thesis is dedicated to,

My Father

Whose dream was to go to my convocation and see me as a Doctor. But no one knew that he time to depart from us is so near. His prayers and love can still be felt from heaven. May his soul rest in peace and may Allah Almighty grant him highest place in Jannah. Amen

My Mother

Who worked very hard with the dream of empowering us with education and make us independent. A bravest soul and role model for us.

My Mentor, My teacher

Who taught us to stand in every difficult situation and never loosing hope. Who taught us to believe in ourselves. Who taught us to strive and work hard. It is due to his guidance and prayers that people consider me a strong-willed person and consider me successful.

ACCEPTANCE BY THE VIVA VOCE COMMITTEE

TITLE OF THESIS:

"ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COMMERCIAL TRANSACTIONS: A COMPARATIVE STUDY IN SHARIAH AND LAW"

Submitted by: Hafsa Abbasi

Reg. No. 23-FSL/Ph.DIJ/F11

1. **Dr. Hafiz Muhammad Anwar**
   Assistant Professor Shariah, FSL, IIUI /
   Supervisor

2. **Dr. Muhammad Asim Iqbal**
   Assistant Professor Law, FSL, IIUI /
   Co-Supervisor

3. **Dr. Samia Maqbool Nayazi**
   Assistant Professor Law, FSL, IIUI/
   Internal Examiner

4. **Dr. Muhammad Moti-ur-Rehman**
   Sr. Advisor,
   Federal Shriat Court, Islamabad/
   External Examiner-I

5. **Prof. Dr. Mohyuddin Hashimi**
   Dean/ Professor,
   Faculty of Arabic & Islamic Studies, AIOU, Islamabad/
   External Examiner-II

External Examiner 2

_____

Declaration

I, Hafsa Abbasi D/O Abdul Rahim Abbasi, Reg. no. 23-FSL/Ph.D/F11, hereby declare that this dissertation entitled "Admissibility of Electronic Evidence in Commercial Transactions: A Comparative Study in Sharī'ah and Law" is original and has never been presented in any other institution. I, moreover, declare that any secondary information used in this dissertation has been duly acknowledged.

Signature _____

Hafsa Abbasi

ACKNOWLEGMENTS

I with all my heart and soul thank my Lord, who gave me strength to undertake this research work and partially contribute towards the diffusion of knowledge on the very contemporary issue of Electronic Evidence.

I am very thankful to my supervisor, Dr. Hafiz Anwar, who gave me time whenever I needed and for helping in Islamic Law Portion.

I am also very thankful to my co-supervisor Dr. Asim Iqbal whose suggestions helped me improve the quality of research. He helped me bring a flow in the contents of a thesis.

I am extremely grateful to one of my friend Rabia Malik, a wonderful researcher and a writer, for proof reading the whole thesis in the end. She not only corrected the construction of the sentences, but also helped me a lot in bringing a flow with in chapters and in between the chapters. I owe her a lot in this work.

I am very thankful to my husband for bearing with me during my thesis and being so supportive. His encouraging attitude towards my project was one of the most essential element towards completion of this project.

I can never forget the help of my eldest two sisters who took care of my kids, during my library hours. It helped me concentrate more on my work and I really enjoyed working on it.

All my family members were are a great help in all respects. I am thankful to all of them. Deep thanks to all those who extended co-operation for the compilation of this work.

My prayers will stay with these people for ever and I will be indebted to them. May Allah reward them in this world and hereafter.

Abstract

The standards laid down for the judge for admitting electronic evidence are still in formative stage, although considerable work has been undertaken, and some provisions have also been made in the laws of different countries including Pakistan , but the law in this area is a work in progress, therefore it is essential to begin judging this form of evidence in the light of the principles of Shariah, in the context of Pakistan, to establish whether the criteria of real evidence and admissibility are met. Electronic evidence is different from physical evidence, whether it be, mode of archiving to display in court, or storage of data. This dissertation analyses the status of electronic evidence from shariah perspective under the topics, documentary evidence, expert testimony and circumstantial evidence. For admissibility of electronic evidence, in English law, this dissertation covers four areas, i.e authentication, relevance, hearsay rule and best evidence rule. Authentication of electronic evidence is a technical process. Different types of evidence need different authentication techniques. Sometimes during authentication process courts require expert testimony. Expert should be qualified according to certain standards applicable world-wide. Electronic evidence is also proved through strong circumstantial evidence which are considered as beyond reasonable doubt. For instance, police get the email address and password from the house of the criminal which was used to commit electronic frauds. While some times cases are solved on the basis of electronic discovery and electronic search and seizures, where electronic evidence becomes strong circumstantial evidence that cannot be denied. Like call record, internet history, finger prints etc. Pakistani law stands equipped for the new times with three modest pieces of legislation, namely Qanun-e-Shahadat Order (Q.S.O 1984), Electronic Transaction Ordinance (ETO 2002), and Prevention of Electronic Crimes Act (PECA 2016). But these laws are not as elaborative on the above mentioned four stages of admissibility as

other laws of countries are. Same is the case with case laws. There is a dire need for policy makers, judiciary and legislatures to work in collaboration to improve the system. Lack of infrastructure and training on the part of investigation officers, judges and lawyers are posing a lot of problems in disposing off such cases. Law of Pakistan need to be updated along with Sharī'ah complaint provisions.

Table of Contents

CHAPTER 1 INTRODUCTION TO ELECTRONIC EVIDENCE

1.1 Introduction

Up until the late twentieth century, computer was the subject of academic discussion and an idea of scientists and inventors under development. It was only in the 1970's and 1980's that computers were introduced in homes and offices.[1] In Pakistan, this technology was introduced even later. At first, the computer was used as a word processor, but in 1996 the whole world changed when the first web-based email service, Hotmail, was introduced.

Since the advent of computers, there have been innumerable changes and advancements in the field of information technology. This advancement reflected in the reformation of organization behaviors. The offices where once, paper was the only medium of record keeping, modernized and the paper-based records got replaced by advanced digital storage systems and records. Surveys now show that almost 90% of the data of different companies and corporations are stored electronically. [2]

Up until the recent past, all our important documents and letters were written by hand, or perhaps typed on a typewriter. Either way, the outcome was a piece of paper. If the paper carried secret information, it could be placed safely in a secure location. Or, if the paper contained some outdated or useless information, it could be destroyed completely by a simple match stick. All of these facts have changed with the passage of time and with the arrival of computer technology. A simple document apparently deleted can be recovered indefinitely if it is in electronic form.[3]

---

[1]Oleh Hryko, *Electronic discovery in Canada: Best Practices and guidelines*, Ed. Richard Browne (New York: CCH Canadian Limited. 2007), 1.
[2] SINTEF. "Big Data, for better or worse: 90% of world's data generated over last two years." ScienceDaily. www.sciencedaily.com/releases/2013/05/130522085217.htm (accessed July 20, 2018)
[3] Ibid

Similarly, twenty years back if one wished to send a letter to a friend residing across the country, he would write a letter and send it through postal service. In case of dispute, the letter was the real evidence, containing major information. The process of investigation, discovery and collection of evidence would revolve around physically existing objects. For instance, cabinets, desks, dust bins etc. [4]

Contrary to the past, letters are sent through the use of the electronic mail today. The letters are only a click away and reach the recipient within seconds. These mails do not exist in the physical world but they have significant value in the virtual world of the internet. In case any dispute arises regarding the matter of such data, the investigation and evidential foundation will be entirely different. For example, search for an e-mail will involve a search of the senders and the recipient's computers. These kind of searches and seizures are different from the presence of fingerprints on the letter, etc. The defendant can also contend that he never wrote or sent that email. So, the question arises as to how will the virtual evidence will be proved and authenticated in the court. This scenario has put the jurors and lawyers in a fix as they are increasingly required to access electronically stored information.

A lot of work has been done in the Western countries, which have critically analysed their own legal framework in the light of the principles of electronic evidence and the rules of admissibility. [5] However, the works are usually confined to their own country's legislation. Thus, there was a need of a research that could analyse and compare the Islamic principles of electronic evidence with western principles of electronic evidence, so that reforms for Pakistan's legal framework can be suggested.

---

[4] Oleh Hryko, *Electronic discovery in Canada: Best Practices and guidelines*, 1.

[5] Jonathan Frieden, D., and Leigh M. Murray. "The admissibility of electronic evidence under the federal rules of evidence." *Richmond Journal of Law & Technology* 17, no. 2 (2011): 5. And Fredesvina Insa, "The admissibility of electronic evidence in court (AEEC): fighting against high-tech crime—results of a European study." *Journal of Digital Forensic Practice* 1, no. 4 (2007): 285-289 and Murdoch Watney, "Admissibility of electronic evidence in criminal proceedings: an outline of the South African legal position." *Journal of Information, Law & Technology* 1 (2009): 1-10.

This dissertation comprises of three main parts following a brief introduction. First part shall deal with Sharī'ah perspective on question of admissibility. This section is dealing with electronic evidence in general. The rest of the thesis will be focusing more on electronic evidence in civil law and commercial transactions. Quoting few examples from criminal laws where appropriate.

The second portion shall deal with Western legal point of view on questions of

admissibility. This part shall be divided into three subcategories. The first sub category is admissibility of electronic evidence, the initial stage. It includes initial questions to be asked by the judge. i.e is evidence relevant? Is it authentic? The second sub category deals with the question of admissibility at the subsequent stage which involves question of hearsay and best evidence rule. The third category is admissibility of electronic evidence at trial stage. The chapter shall deal with how electronic evidence will be dealt under civil as well as criminal law. Last part of this section is the only one which is specifically dealing with criminal law under topic electronic search and seizure.[6]

The third part of this thesis shall discuss Pakistani law relevant to electronic evidence. In this section special focus is on commercial transactions as two main initial laws of Pakistan, till 2016 were generally based on electronic commerce. These were Electronic Transaction Ordinance 2002 and Qanoon-e-Shahadat order 1984. Later Prevention of Electronic Crimes Act was passed in 2016, which is about cyber-crimes. Major sections of ETO, and QSO which relates to commercial transactions, like electronic data, electronic signature, advanced electronic signatures, electronic transactions and certificate service providers have been discussed in this chapter.

---

[6] See chap. 5, para 5.2.

At the end, a detailed comparison of three legal systems i.e Islamic, Western and Paksitani legal system, shall be drawn out which will help highlight the gaps in the legal system of Pakistan.

This chapter is primarily focussed on the introduction of e-evidence. The basic definitions and terminologies relevant to e-evidence shall be discussed here. This chapter will further proceed on to briefly discuss the main frame of ideas which will be taken up in the rest of the thesis. The first step in this regard is to discuss the importance of digital evidence in crimes and investigation.

1.2 Thesis Statement

The standards laid down for the judge for admitting electronic evidence are still in formative stage, although considerable work has been undertaken, and some provisions have also been made in the laws of different countries including Pakistan , but the law in this area is a work in progress, therefore it is essential to begin judging this form of evidence in the light of the principles of Shariah, in the context of Pakistan, to establish whether the criteria of real evidence and admissibility are met.

1.3 Objective of the research

This research would aim to explore

1. *Sharī'ah's* perspective on electronic evidence.
2. The standards of admissibility for electronic evidence in Islamic law as well as US Law.
3. Reviewing cyber laws of Pakistan, analyse the weaker areas and comparing them with laws of USA.

4. To analyse local (Pakistan's) legal scenario on electronic evidence from the perspective of Islamic law.
5. Comparing all the three systems, western, Islamic and Pakistan for suggesting changes for Pakistan.

1.4 Methodology of the Study

Research methodologies applied in this research will be analytical and comparative. Library sources will be utilized in this research extensively. References will include excessive literature in the form of text books, articles, reports, statutes and decided cases. Research on *Sharī'ah* will be based upon Qur'ān, *Sunnah* and the traditions of Prophet's companions. Work of classical Muslim jurists will be used as primary sources in this research. The classical textbooks as well as contemporary work of Muslim scholars will be utilized on the said subject. Any direct material is not available on this topic in classical Islamic law, however, traditional principles of law of evidence shall be applied on electronic evidence, trying to make analogy, different rules shall be derived for current situation. Contemporary scholars who contributed on this subject are mostly confined to permissibility of electronic evidence only. But this research aims to dig deeper into the layers of *Sharī'ah* in order to discover the theories on Islamic law for evidence and derive rules for electronic evidence. Major work in this thesis will be of extraction and derivations.

This research will be descriptive as far as the theory of law of evidence in *Sharī'ah* and law are concerned. Further, it will explore, review and analyse current laws on electronic evidence in USA and then in Pakistan. This research will be analytical.

It will be a qualitative research and will explore the advancements in the law of electronic evidence and need to incorporate certain changes in Islamic law.

1.5 Scope and limitation of the Study

This study is focused on basic principles of admissibility in Islamic, Western and Pakistani law. Means of proofs, in Islamic law are discussed with special focus on documentary evidence, expert testimony and circumstantial evidence. Law relating to Commercial transactions are also discussed side by side. For instance, authentication of electronic data, law of electronic signatures, Electronic Transaction Ordinance 2001. Electronic discovery in civil cases and criminal search and seizure are also discussed to show how electronic evidence works in court.

As per the title of thesis, the detailed laws of commercial transactions like, sale, pledge, insurance, carriage by road and rail, details of electronic contracts, and their payment methods will be discussed. But these are out of scope of this thesis. As it is confined to principles of admissibility.

1.6 The Importance of digital evidence in Trials and Investigation

Electronic evidence is considered to be the most important aspect of a criminal as well as well as commercial transactions. In fact, in the present times, it is very difficult to solve a case whether criminal or civil without electronic evidence. A bulk of cases are there to support the argument. Some of them are discussed here.

In criminal cases, case of Philip Welsh can be a good example, who worked as a taxicab dispatcher in Maryland, he had the habit of using technology and computers in office, on daily basis. But never used such devices at home and in private life. On February 2014 he

was murdered in his home. Welsh, never used cell phone or PC, but relied on landlines, handwritten letters and typewriters. He was a happy person without modern gadgets. Friends and family prompted him to start using such things but Welsh preferred being simple and never came in touch with internet and social media. When he did not come to work from home where he lived alone and there was no proof that he had enmity with anyone. In fact, he was a well-liked person. Usually he permitted taxi drivers to use his house for sleeping between shifts. The lack of digital evidence in this case served to be a big hurdle in investigating the causes of crime. Police had no way of finding out Welsh's activities, what he was involved in or whom he met or was planning to meet before murder. Here there is a strong need felt by the investigation officers to have traces such as text messages, mails and browser history. This murder remained unsolved and investigation officers noted that this happened due to the lack of digital evidence.[7]

Another case, in which electronic evidence played a vital role was when Christian Aguilar disappeared on September 2012. He was a freshman at university of Florida and had been in friendship with Pedro Bravo, since eighth grade. Christian Aguilar was last seen with his friend, Bravo. Three weeks later, Aguilar's dead body was found from a shallow grave almost 60 miles away in the west. Police suspected Bravo had some link with the disappearance and death. After search it was found that he was in possession of Aguilars' backpack. The reason why Bravo was upset with Aguilar was that Aguilar had started a relationship with Bravo's ex-girlfriend. Hence, digital evidence made this circumstantial case far more certain. Electronic evidence experts had access to Bravo's cell phone and got many

[7] Sean E. Goodison. Robert C. Davis. and Brian A. Jackson. "Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence" Rand Cooperation, 2015, 3. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf. (accessed. May 9. 2017) Also in. Dan Morse. Philip Welsh's simple life hampers search for his killer. Washington Post. May 6. 2014 https://www.washingtonpost.com/local/crime/philip-welshs-simple-life-hampers-search-for-his-killer/2014/05/05/1fd20a52-cff7-11e3-a6b1-45c4dffb85a6_story.html?utm_term=.cc88146e147f

key pieces of proofs. Examiners found out that in the cache for the phone's Face book app, there was a screen shot of a Siri search made near the time of Aguilar's disappearance that read, "I need to hide my roommate." Determining the tower that received signals from the cell phone, which showed that Bravo had moved far to the west after the disappearance. In the end, examiners were able to investigate that the flash light app on the cell phone was used for almost one hour after the disappearance. After gathering these evidence and proofs, Bravo was tried in the court in the light of these circumstantial evidence. Bravo confessed his crime and in August 2014 he was convicted of first-degree murder.[8]

Same is the case with civil trials and commercial transactions. These days most of the people make electronic contracts, use electronic signatures and save huge volumes of electronic data on computers. Big business corporations has the legal duty to keep the data safe, reliable and accessible. Otherwise, it is going to cost them a fortune because corporations are bound to recover any disputed email or electronic record demanded by court in case of need. [9] So the electronic evidence from commercial transactions has prime importance.

Law of electronic commerce is primarily derived from UNCITRAL model laws of electronic commerce 1996 and UNCITRAL model laws of electronic signatures 2001. Most of the states including Pakistan adopted these guidelines in order to come in par with international standards of e-commerce. Pakistan's law dealing with commercial transactions

---

[8] Sean E. Goodison, C. Davis. Robert, and A. Jackson. Brian. "Digital evidence and the US criminal justice system." 3. Also in Lauren Effron, Jim Dubreuil And Laura Ramirez "Girlfriend at Center of Gainesville Love Triangle Never Thought Killer Ex Was Capable of Murder " New York. ABC news. Aug 20, 2014. http://abcnews.go.com/US/girlfriend-center-gainesville-love-triangle-thought-killer-capable/story?id=25060406

[9] Zubulake case. *Eckhardt v. Bank of America Corp.*, 2008 WL 1995310 (W.D.N.C 2008)

is ETO 2002. It discusses electronic contracts,[10] electronic signatures,[11] certificate Service providers, authentication of electronic contracts and records. [12]

Electronic evidence whether for commercial transactions or criminal cases, has existed for decades in limited forms, such as mainframe computers and telephonic systems, the importance of processing digital evidence has increased with advancements in mobiles and computers. It was observed by the supreme court of USA that these days mobile phones are not only phones but mini computers, which serve as a microcomputer, telephone, calender, diary etc.[13]. On-line shopping is done through cell phones, internet history can reveal a lot of things regarding any crime committed. Text messages, what's app chats, call records and messages record can recover large amount of essential evidences.[14]

1.7 Background and Significance of Study

Field of electronic evidence established its roots in the Western legal system hardly two three decades ago. This area has greatly increased and given birth to huge volumes of data in corporations. It has also resulted in innovating new technologies like cloud computing etc. Main source of transferring information and communication is internet. Recent studies show that there is a drastic change in mode of shopping. Most of the people are choosing to opt e-commerce. Large organizations prefer to make commercial transactions on-line. For instance, banks order large machines demanded by the customers on-line (letter of credit).

---

[10] See chap 6, para, 6.3.1.
[11] See chap 6, para, 6.3.1.1.
[12] See chap 3, para, 3.1.
[13] Riley v California, 573 U.S __ (2014). (Accessed: May 9, 2017) https://supreme.justia.com/cases/federal/us/573/13-132/
[14] Goodison, Robert C. Davis, and Brian A. Jackson, "Digital Evidence and the U.S. Criminal Justice System", 5.

US department of E-Stat states in a report that 93% of manufacturers and merchants (called B2B) are using e-commerce.[15] A survey in china showed that till 2009, 74 million people used on-line shopping.[16] Different States all over the world incorporated the laws of electronic commerce which are mostly derived from United Nations model laws on electronic commerce and electronic signatures.

Pakistan also did the same, in the form of Electronic Transaction Ordinance, 2002. But apart from this basic law some advanced legislations are strong need of time. But unfortunately, that process is slow here. For instance, Prevention of Electronic Crimes Act was enacted in 2016. Although the drafts and preparations were made since almost 2008 onwards. Another problem with the legal system of Pakistan is that it is based on English laws enacted before independence. For instance, in case of law of evidence, Pakistan followed Evidence Act 1872 till 1984. After that Qanun-e-Shahadat 1984 (Q.S.O) Order was enforced repealing previous Evidence Act 1872. But the truth is that, Q.S.O is a mere repetition of Evidence Act 1872 except article 3, 4 to 6 (with reference to Hudud), adding article 44 and addition of a proviso to art 42.

So, the focus of this dissertation will be to analyse Islamic law of evidence, in order to apply those principles to electronic evidence by way of analogy. Based on the analysis certain recommendations will be suggested for Pakistan's legal system. But before that US law, which is most advanced in terms of availability of case laws and latest literature, shall be explored in detail in order to have a picture of world's best practices in the field of electronic evidence.

---

[15] Faye Fangfei Wang. *Law of electronic commercial transactions: Contemporary issues in the EU, US and China* (Routledge: New York, 2014), 3.
[16] Ibid.

This thesis is going to dig out the principles from Sharīah applicable to e-evidence. As, there are no direct rules addressing e-evidence. Existing laws of Pakistan which are mostly relevant to commercial transactions (e-commerce) shall be analysed in detail with the help of case laws.

Previous researches done in this area are not addressing these issues from the perspective mentioned above. This thesis will discuss three legal systems (Islamic, Western, Pakistani) and compare them in the last chapter. Existing Researches in Sharī'ah regarding electronic evidence or mostly based on fatāwas about the permissibility and admissibility of e-evidence. For instance, fatwa on the permissibility of emails, text messages, etc. Less research is done in detail aiming at exploration of the principles and philosophy of Islamic law of evidence, for the purpose of applying them to modern means of proofs and evidence.

Western laws on the other hand, is quite advanced in electronic evidence. A large number of books, articles and blogs are available, both on-line and libraries explaining different angles and issues of electronic evidence. However, most of the researches are confined to the particular legal systems of the countries addressed by the authors, like, USA, U.K, India Singapore etc. So, comparing the three legal systems i.e. Islamic, Western, and Pakistani law was need of the hour. This thesis will serve to be a base for future research on laws of e-evidence in Pakistan.

1.9 Varying Status of Courts

The recent times have seen an explosive growth in electronic commerce (e-commerce). Electronic evidence (E-evidence) arising from this field has different forms such as data files, internet postings, emails, etc. It can be acquired from many areas and can come in the form of 'background' information, like audit trails, access control data, and other non-printed

information etc. E-evidence can also be a type of residual data, which remains on the hard drive even after being deleted, or in printer and fax memories.[17]

Initially, the courts were reluctant to rely on electronic evidence due to diversity in the nature of electronic evidence. Nature of ESI (Electronically stored information) shows that it can be tampered very easily. Digital malfunctioning occurs quite often and errors are faced quite often in different software programmes. Electronic evidence can be altered very easily. Hacking of different accounts and making embezzlement is a common practice too. Anyone can write anything on the Internet. Website postings, face comments, chatting, etc. are common examples.

Due to these reasons, on numerous occasions, the courts highlighted the risks involved in trusting electronic information. In a number of cases, courts illustrated the dangers inherent with electronic evidence and the reluctance of courts to admit it as evidence at trial. For example, in *Lee v. Oracle Corp. Inc.*, 1997[18], the plaintiff employee, Lee, was using e-mail as evidence and showed that she had been fired after breaking off an illicit affair with her boss. While this evidence initially seemed damning, it was later shown that Lee had hacked into her employer's e-mail account, and had written the e-mails herself. Perhaps, such fraudulent activities motivated the court to reject electronic evidence outright. For instance, in *St. Clair v. Johnny's Oyster & Shrimp*, [19] the court rejected the information retrieved from the internet. The Court referred the information posted on the internet as "inherently untrustworthy". The judge in this case refused to accept records that had been gathered from the websites and was of the view that anyone can put anything on the internet. Hackers can adulterate the content of any website from any location at any time. Evidence procured off the internet is adequate for almost nothing'.

---

[17] Paul. P. Rice, *Electronic Evidence: law and Practice* (New York: ABA Publishing, 2005),1.
[18] WL 257214 (Cal. Ct. 1996), see Hryko, *Electronic discovery in Canada*, 177.
[19] Inc., 76 F. Supp. 2d 773, 774 (S. D. Tex. 1999)

The court held in this case:

> Plaintiff's electronic 'evidence' is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumour, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules in FED. R. EVID. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form from the United States Coast Guard or discover alternative information verifying what Plaintiff alleges.

Thus, the court in the above case refused to accept records that had been gathered from the U.S Coast Guard's online vessel database, on the above-mentioned grounds. But due to the inevitable role of electronic data in our daily lives, these views could not last for long. Judges had to change their strict stance of rejection and not be so harsh with electronic evidence. For instance, in the case of *Telewizja Polska U.S.A, Inc. v. Echostar Satellite Corp.*[20], the court held that copies of a website archived by the Internet Archive's Way Back Machine[21] were admissible as authentic copies of the website at issue. The court also held that the printout of a website is admissible pursuant to the best evidence rule.

---

[20]2004 WL 2367740 (N.D.III. Oct. 15, 2004)

[21] The Way back Machine is a digital archive of the World Wide Web and other information on the Internet created by the Internet Archive, a non-profit organization, based in San Francisco, California, United States. The overall vision of the machine's creators is to archive the entire Internet. The authorities of this machine say "The Internet Archive is working to prevent the Internet - a new medium with major historical significance - and other "born-digital" materials from disappearing into the past. Collaborating with institutions including the Library of Congress and the Smithsonian, we are working to preserve a record for generations to come". accessed 23rd January, 2017.
https://archive.org/web/collaborations.php

Similarly, in other type of evidences courts had to adopt a lenient stance. For instance, when e-mails and other electronic communication was presented in court for evidence the court held, in both *re F. P*[22] and *People v. Downin*[23] that they are admissible pieces of evidence. Courts refused to impose any special burden on those seeking to introduce e-mails or instant messages as evidence. In both the cases, the court held that expert testimony is not needed. It declared the email at issue, as sufficiently authenticated by circumstantial and other evidence.[24]

The reason behind the change of court's rigid behaviour towards e-evidence into a flexible one is that it is not always the case that the emails are fabricated and identities are hacked. It happens sometimes and can be cured. Another factor which helped in developing the trust of courts on these means is the great degree of society's trust on emails and messages in their ordinary course of business. It was held by the court that it is nonsensical to believe that emails are not capable of being trusted because identities can be hacked. The reason given by the judges was that even the hand written letters posted through postal services can be fabricated or the signatures of a person can be forged. But this does not lead the court to completely reject the credibility of all such means. So, with the use of e-evidence, apprehensions are always there but they can be cured and investigated. [25]

1.10 Definition of Evidence

"Evidence can be defined as the means employed for the purpose of proving an unknown or disputed fact". It can be judicial or extra judicial. Every result of the judgement,

[22]878 A.2d 91 (Pa. Super. Ct. 2005)
[23]828 N.E.2d 341 (III. App. Ct. 2005)
[24]Hryko, *Electronic discovery in Canada*, 42.
[25]Stephen Mason, *Electronic Evidence*, 137.

irrespective of the subject matter, is based on the evidence. [26] Word evidence refers to any information upon which a person can base a decision. For instance, if a person is interested in purchasing a car, he will first visit the owner of that car to gather basic information. Later on, the seller would go to some mechanic to check the condition. A decision of buying or not buying the car shall be made on the basis of evidence gathered.

1.10.1 Legal Evidence

The term legal evidence is defined in Black's law dictionary as "all the admissible both oral and documentary of such a character that it reasonably and substantially proves the point rather than merely raising suspicion or conjecture". [27]

Legal evidence is the one which is used at trial or inquiry before the judge, jury, court or commission. Legal evidence can also be defined as "evidence which demonstrates or makes clear or ascertains the truth of the very fact or point in issue, either on the one side or the other."[28]

Evidence is the study of information through which facts can be proven. The law of evidence on the other hand, is that body of law which regulates the means by which facts can be proven.[29] It is not purely substantive law, rather it overlaps with procedural law. The broad governing principles of evidence in English Law about the admissibility can be explained in nine words; all the relevant evidence is admissible, subject to the exceptions.[30]

---

[26] Jefferson L. Ingram. *Criminal Evidence*. 12th ed. (Waltham: Anderson Publication, 2015). 24.
[27] Black's law dictionary 9th ed. S.v. "Evidence".
[28] Leonard v. State, 100 Ohio St. 456. 127. N.E 464 (1919). quoting Black Stone (Blackstone's Commentary). Also in Ingram. Criminal evidence. 40.
[29] Adrian Keane and Paul Mckeoron. *The modern law of evidence* (New York: Oxford University Press. 2014). 1.
[30] Ibid

Law of evidence can also be defined as a "system of rules for ascertaining controversial questions of facts in judicial inquiries". The object of every judicial proceeding is the enforcement of any right or liability which invariably depends upon certain facts.[31]

1.10.2 Admissibility of Electronic Evidence

The concept of admissibility determines that evidence can be accepted by the court. Admissibility is the concept which discusses the criteria of evidence, accomplishing which, evidence can be received by the court.

Admissible evidence is also called proper and competent evidence. Black's law dictionary defines competent or admissible evidence as "evidence that is relevant and is of such a character (e.g. not unfairly prejudicial or based on hearsay)"[32]

The word admissible is defined by the same dictionary as, "pertinent and proper to be considered in reaching a decision, used with reference to the issues to be decided in any judicial proceeding. In case of evidence, this term refers to the evidence of such a nature and character which the judge or court is bound to revive, which means allowing it to be introduced.[33]

Admissible evidence is competent evidence which can perhaps be understood better if the definition of incompetent evidence is looked at; "evidence that is for any reason inadmissible" [34]

---

[31] M. Monir, *Text book on the Law of Evidence* (New Delhi: Universal Publishing co., 2010), 1.
[32] Blacks law dictionary s.v. "admissible evidence".
[33] Ibid
[34] Ibid, s.v "incompetent evidence"

Whenever an evidence is presented before the court, its competency is checked. If the evidence is not proper or it has some defects, it is considered inadmissible. There are so many examples in law as well as in Islamic law when the cases were proven against the offenders but punishment had to be stopped because the evidence was not properly authenticated. For instance, Kentucky court declared that the evidence was defective and improper although the proof declared that the accused was a felony offender. The punishment had to be stopped because the evidence was not properly authenticated and the evidence introduced against defendant was incompetent. [35]

There are a number of questions regarding the competency and admissibility of electronic evidence. Volumes of data is available on what kind of evidence is admissible. But the questions of admissibility of electronic evidence from the perspective of Islamic law and its application on Pakistani law, are new and need to be researched.

This thesis is aimed at answering the question of admissibility of electronic evidence in three legal systems. Firstly, to check the admissibility of electronic evidence in Islamic law. Secondly, check admissibility of e-evidence in law and thirdly to check admissibility of e-evidence in Pakistani Law. All three perspectives are explored in separate parts of this thesis.

1.10.3. Commercial Transactions

The term Commercial transaction is defined as "the core of the legal rules governing business dealings. The most common types of commercial transactions, involving such specialized areas of the law and legal instruments as sale of goods and documents of title"[36]

[35] Jefferson L. Ingram, Criminal evidence, 12th ed. (Waltham: Elsevier, 2015), 250.
[36] "*Commercial transactions*" *s.v Britannica.* https://www.britannica.com/topic/commercial-transaction (Last Accessed July 11, 2019)

Term electronic is defined by Economic Co-operation and Development (OECD) as;

"All forms of commercial transactions involving both organisations and individuals, which are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may have on the institutions and process that support and govern commercial activities." [37]

1.11 Admissibility of Electronic Evidence in Islamic Law

As far as the question of admissibility in Islamic law is concerned, it is a thorny question because there are no direct proofs to this question. In the classical Islamic law, however, indirect proofs are available. These issues are addressed in detail in the second chapter.

The question of admissibility of electronic evidence in Islamic law needs an overview of Islamic law of evidence in general. Only then it can be checked against the criteria of admissibility. Chapter two explores the question of admissibility of electronic evidence through discussion of seven means of proof in Islamic law. They are as follows:

1. Al-Yamīn (Oath)
2. Al-Iqrār (admission/confession)
3. Al-*Shahādah* (testimony)
4. Al-Kitābah (documentary evidence)
5. Ra'yu al-khabīr (expert opinion)
6. Al-*Qarīna* (circumstantial evidence)
7. 'Ilm al Qāḍī (knowledge of a judge)

[37] Faye Fangfei Wang, *Law of electronic commercial transactions: Contemporary issues in the EU, US and China* (Routledge: New York, 2014), 5.

Among all these means, four means of proof are discussed in detail because they are closely related to electronic evidence.

1. Documentary evidence
2. Testimony (*Shahādah*)
3. Expert Testimony
4. Circumstantial evidence (القرائن)

A short discussion of the above mentioned four means of proofs is presented to provide a basic introduction of the means.

Oral Testimony

There are two types of oral testimony in English law as well as Shar'iah

1. Witness with knowledge
2. Expert witness

The Common law requires oral testimony on electronic evidence.[38] The data whose content is already proven requires a witness with knowledge.[39] For instance, in authentication of business records or computer records, a custodian of these records needs to testify in order to prove the safe custody and integrity of the evidence.[40]

[38] Oral testimony is a must where the content of a document is not proved. But when the content of data is not disputed, electronic evidence is admissible without oral testimony. For instance, Section 22A of Indian Information Technology Act says that oral testimony is not required where the content of data is reliable. Accessed May 25, 2017. www.aicle-inida.org/downloads/itact2000pdf. is the one which is self-authenticating like public document or business record. The chain of custody and reliability of such document is established. That is why oral testimony is not required here.

[39] See chap 3, para 3.3.4.1 authentication by witness with knowledge.

[40] See chap 4, para 4.2.3.1.

But in case where programming and certain codes are involved, the authentication of that software is essential. The writer of the software code shall testify in that case.[41] Similarly, matters where computer forensics are involved or require special knowledge and expertise; expert testimony is adduced. Expert testimony is required in the cases where the matter to which the material relates is beyond the ordinary human experience. Both these testimonies; oral and expert are analysed in Islamic law to build room for comparison in the minds of readers.[42]

In English law Daubart and Fryer were the precedents which were followed for a long time in order to decide whether expert testimony is required or not. While in Islamic law there are different precedents from Prophet (PBUH) and Companion of Prophet (PBUH) where they took help from relevant experts from different fields.[43]

The means of proof in Shari'ah have quite much in common with English law. They are almost the same. Islamic law is older and has been more functional and experienced. [44] It can be said that means of proof in English law (which are called means of authentication in common law) are derived from Islamic law.[45]

There are seven means of proof in Islamic law, as mentioned earlier. These means are the same with a little difference in the English Law.

Islamic law requires oral testimony and English law offers the same. Islamic law has relied upon expert testimony, confession and circumstantial evidence. All these are equally acceptable in English law.

---

[41] See chap 4, para 4.2.2.2.
[42] For details of expert testimony see chap 2, para 2.3.5 and for the details of Oral testimony, see chap 2, para Oral testimony is discussed in 2.3.3.
[43] See Chap 2, para. 2.3.5.
[44] It has experienced its rule and glory for more than 110 years as Umayyad, Abbasids and Ottomans. Ottomans had a downfall took place around in 1918-1920
[45] See chap 3, para 3.4.

For instance, there is ample discussion regarding the documentary evidence in Islamic evidence. Electronic evidence is documentary and there is no confusion about it. [46] This mean of proof is common in Law and Sharī'ah.

The following section discusses the four steps or stages of checking admissibility of evidence.

1.12 Admissibility in US Law

After addressing the question of electronic evidence's admissibility in Islamic law, the dissertation analyses the question of its admissibility in the western legal system. The definition of admissibility, as discussed earlier, states that during the procedure of checking the admissibility of evidence, the court looks for certain requirements which must be present in an evidence.[47]

1.12.1.1 Stages for Admissibility

For the purpose of admissibility, the western legal system requires four criteria to be satisfied. Only then the evidence is admissible or competent. Following are the three stages of electronic evidence. The details of the stages shall be presented in the upcoming chapters. The three stages are:

1. Electronic Evidence; the initial stage. It discusses initial steps of admissibility, i.e. relevance and authentication.

[46] All the states have legislated in a way that they have expanded the concept of documentary evidence to electronic evidence as well. Pakistan is also an example in this regard, article 2(b)of Qanoon-e-Shahadat Order state that document can be a letter, figure, photograph or words printed. Due to this many judgments in Pakistan have linde article 2(B) with article 164 of Qanoon-e-Shahadat Order and said that the word document is implied to the evidences that are available because of modern devices. One of the leading cases in this regard is *Sikandar Ali Lashari v. The State* (2016) YLR 62 KARACHI HIGH COURT SINDH, it was observed that the term document is expanded and includes CDs Usbs and other electronic evidences. See chap 6, para 6.3.3.

[47] See Chap 3, Para 3.3 and 3.4 Also see Chap 4, para 4.2 and 4.3

2. Electronic Evidence; the subsequent stage: It discusses the later stage which involves scrutiny of hearsay and best evidence rule.
3. Electronic Evidence; the trial stage: At this stage the practical implication of electronic evidence in courts is checked. It is further divided in two parts; one discusses electronic evidence in civil trial, while the other discuss electronic evidence in criminal trial. [48]

To have a better understanding of admissibility stages of electronic evidence, classification of electronic data needs to be understood.

1.12.1.2 Electronic Data Classification

The problem of authentication arises when different kinds of data are to be dealt with. Mainly, the data on a computer can be classified into three types:

a) Computer generated data: It is the data which is generated by a computer without human intervention.[49]

b) Computer stored data: It is the type of data which is stored on a computer. In this type of data, computer only serves as a cabinet or folder. The data entered into it, is created manually. In this situation authentication of data by a person who entered the data are required. [50] Authentication of computer stored data is a task usually accomplished by oral testimony of the relevant person, i.e. the person who entered the data or who is familiar with the procedure of keeping and storing the data. Such witness is called "witness with knowledge.

---

[48] See Chap 5, Para 5.1 and 5.2
[49] See chap 3, para. 3.4.4.1.
[50] See chap 3, para 3.4.4.2.

c) Mixed data: It is the type of data which contains both computers stored and computer-generated data. Authentication of this type is different. [51]

The solutions to the authentication issues related to the three classes of data mentioned above are discussed in detail in chapter 3 of this thesis work, under the topic of authentication.

1.12.1.3 Relevance (Stage I)

The first criteria of is the requirement of relevance.[52] The evidence must be relevant to the facts. This means that the evidence must have the capacity to make the acts either more or less probable.

1.12.1.4 Authentication (Stage I)

The second admissibility criterion is authentication. It is the stage when unreliable evidence is excluded from the trial. [53] In this stage proponent must be able to establish that "the evidence is sufficient to support a finding and the matter in question is what it claimed".[54]

Authentication of electronic evidence involve a wide range of problems, the most important being the multifarious kinds of electronic evidence. For instance, USBs, hard drives, clouds, databases, servers controlled by internet, emails, web page, instant messages, etc. Each one of the types has a different method of authentication. For instance, authentication of a web page is different from the authentication of emails.[55]

1.12.1.5 Hearsay Rule (Stage II)

It is the third step for admissibility of evidence. The Proponent is bound to establish that the evidence presented before the court is not hearsay. If the evidence is hearsay, the general rule

---

[51] See chap 3, para 3.4.4
[52] See chap 3, para. 3.3
[53] See chap, 3 para 3.4.
[54] Searching and seizing computers and obtaining electronic evidence, 197.
[55] See chap 3, para 3.4.6.

is inadmissibility of that particular evidence. The only exception to this rule is that it must fall under one of the exceptions to the hearsay rule.

A number of exceptions to the hearsay rule are present in common law, which are discussed in chapter 4. For instance, public document and business record.

When the problem of hearsay is discussed in the context of electronic evidence, the issue becomes complex. The reason being, as mentioned earlier, statements which are stored in a computer by a human being would fall under hearsay. [56]

Here, in order to avoid problems of hearsay, the person who stored the data on a computer has to come to the court to testify, or the data stored in the computer must come under any one of the exceptions to the hearsay rule, like, business record or public document.

1.12.1.6 Best Evidence Rule (Stage II)

The last step for the admissibility of electronic data in the court of law is the best evidence rule. It was previously known as original writing rule. It means that a document presented before the court must be original, primary and best possible evidence. [57] The concept was very important in case of physical evidence, but in electronic evidence this rule has completely abolished.[58]

The four steps for admissibility of electronic evidence in common law system have already been discussed. These steps are a mandatory requirement or a pre-requisite to

---

[56] See chap 4, para 4.2.2.

[57] The details of this topic is discussed under the topic Best evidence rule in electronic evidence 4.3.

[58] Majority of the states have legislated that all the documents generated from a computer are primary evidence. Whether, they are hundreds in number. The case was opposite in physical evidence, where there was only one primary evidence and copies or duplicates of it were considered secondary. But electronic evidence has totally rejected the rule that is why all evidence are best evidence which are generated by the computer. Subject to the authenticity and reliability of the system which generated the document.

electronic evidence. But the practical implication of these four steps would still remain unexplored if not discussed in this dissertation.

1.12.1.7 Practical Implications (Stage III)

Practical implication refers to how electronic evidence works in the civil and criminal trial.

In civil trials involving electronic evidence, the issue of electronic discovery is considered to be of the highest urgency. It is excessively researched and legislated by the legal system from all around the world. Legal system of Pakistan, however, stays silent on this topic. The practical implication of electronic evidence in a criminal trial is not an easy task either. The investigation officers face a number of issues such as jurisdictional issues. For instance, a cyber-crime if committed from one corner of the world will have to be traced and the data will be required from that particular country in which the crime was committed. This requires an effective collaboration between the states on this issue. Secondly, seized material from a crime must be handled with care because little negligence can cause grave consequences. Another very important issue which is prevalent in electronic evidence in criminal trial is that of search and seizure. The data which is received by the investigation officer must not be acquired through privileged communication. The search must come under the category of reasonable search. It means that the data acquired must not be without warrant. [59]

1.13 Admissibility in Pakistan Law

Addressing the issue of computer evidence admissibility in Pakistani courts, would require investigating the Pakistan's legal system.

---

[59] See chap 3, para 5.2.

The issue of admissibility of electronic evidence under Pakistan's legal system is not easy to answer because the legal system of Pakistan is far more behind than the developed countries. The legal systems of the world have moved beyond the simple scenario of "electronic evidence is admissible". [60] Majority of the countries have updated their legal systems to cope with the demands of today's high-tech societies.

Pakistan has accomplished the level of "electronic evidence is admissible" but the next step is still under progress and it requires attention of the law making and law enforcing agencies. The next step is to define how the electronic evidence would be entertained in the courts, and what procedure would be followed. Although the legal system of India, USA are much developed in this regard, the legal system of Pakistan is silent about the procedural details.[61]

So, by analysing the Islamic and Western legal systems, some recommendation can be proposed for the legal system of Pakistan, which is still in its infancy state with regards to matters related to electronic evidence.

A comparative analysis between the three legal systems i.e. U.S, Islamic Law and Pakistani law, will be presented in order to propose some recommendations for Pakistan.

After a detailed analysis, in Islamic and US law context, this thesis will discuss the status of Pakistani law, on the following areas;

1. Relevance.
2. Authentication.
3. Hearsay.

[60] Electronic Transaction Ordinance 2002 and Qanoon-e- Shahadat Order are dealing with e-evidence by an approach which only says yes e-evidence is admissible.
[61] See Indian Information technology Act 2000 USA's Federal rules of evidence.

4. Best Evidence Rule.

5. Documentary evidence.

6. Oral testimony.

7. Expert testimony.

8. Qanun-e-Shahadat Order 1984.

9. Electronic Transaction Ordinance 2002.

10. Prevention of Electronic Crimes Act 2016.

Point number 8 to 10, are names of laws of Pakistan that are dealing with electronic evidence and cyber-crimes.

This dissertation will serve as to analyse the status of Pakistani laws on admissibility of electronic evidence. Before that overview of Western, and Islamic legal principles on electronic evidence is given. Last chapter is concluding the whole research along with comparison in between the three systems and suggesting some recommendations in the light of developed laws. All the areas mentioned above are open for the future research in detail, with reference to Pakistani law.

1.8 Literature Review

Literature on the current subject will help to get a picture of existing status of digital evidence around the globe. So that the significance of this research can be highlighted and lacking areas on this subject can be indicated for future research.

Islamic Law

The Islamic law of evidence is a significant field and many worthy Jurists have dealt with the issue of evidence arduously. There are numerous books shedding light on general principles of law of evidence laid down by the *Qur'an* and *Sunnah*. Literature on electronic evidence, however, is scarce. This section mentions a few of the notable works available in the domain of evidence.

Imām Sarakhsī[62] has compiled principles of Islamic law of evidence in his worthy book al-*Mabsūt*,[63] under the title *kitāb al-shahadāt*. The main focus of *Imām sarakhsī* is to teach his disciples techniques of getting flawless and authentic evidence. Most of the principles relating to principles of Islamic law of evidence are discussed in *kitāb al-shahadāt*.

Imām Kasāni is also one of the most eminent scholars of *Ḥanafī* school. His book *Badāi' al-Sanāi'*[64] and *kitāb al-Shahadāt* is a collection of detailed principles of testimony. He has explained this area in depth. Most of his research in this area is from the perspective of

---

[62] Muḥammad b. Aḥmad b. Abī Sahl Abū Bakr, Shams al-'imma al-Sarakhsi, is a great Ḥanafī jurist of the 5th /11th century, who lived in Transxania. Sarakhsi is known for his scholarly commentaries on great books of Ḥanafī School, especially books of *Muḥammad* al-Shaybani. His al-Mabsut, commentary on al-Siyar al-Kabīr and the book on Usul al-Fiqh are Magnum Opuses in the *Ḥanafī* jurisprudence. He died around 490/1096.

[63] Muḥammad bin Aḥmad bin abī Sahl shams al-'Āa'ema al- Sarakhsī. *Al- Mabsūt*, 30 vols. (Beirut: Dār al-Ma'rafa, 1993)

[64] 'Alā' *al-Dī*n Abu Bakr bin Mas'ud bin 'Aḥmad al-Kāsānī. *Badā'i' al-Ṣanā'i fī tart īb al-sharā'i*, (Dār al-Kutub al-'Ilmīah,) 2nd ed 1998, 7 vols.

different conditions of testimony.*Imām Marghinanī*[65] ( ) has given a brief yet very compact insight into the Islamic law of testimony.

Function of Documents in Islamic law [66] by Jeanette Wakin is another very important resource on the background of *shuruṭ* literature in English. It helps getting an idea on the status of documentary evidence in the classical Islamic period.

From among many books and articles on expert testimony, one significant work is Ron Shaham's Expert Testimony.[67] It is a collection of different examples relevant to consultation of expert witness in classical as well as medieval times. Although the book does not provide information in a chronological order, it still gives a good insight of the role of experts in Islamic law.

Circumstantial evidence (*Qarīna*) is quite interesting and helpful field in Islamic law which helps solve the riddles of electronic evidence in Islamic law. An important book of worthy jurist 'Ibn-Qayīm, al-Jaūzīah, titled "Al-Turuq al-Ḥukmīyah fī al-Siyāsah al-Shar'īah" [68], gives a brief overview regarding the legal validity and status of circumstantial evidence in Islamic law.

Circumstantial evidence derived from the modern means of proofs is discussed by 'Adnān Ḥassan 'Azāīza, titled "Ḥujjīah al-Qarāi'n fī Sharī'ah al-Islāmiah al-basmāt - al-kiyāfah - dalalāt al-'asar-teḥlīl al-dam".[69] This book gives detailed account of circumstantial evidence. The author has tried to cover many issues related to circumstantial evidence. It is one of the

---

[65] Burhān al-din abu al-Ḥassan 'Ali ibn abī bakr farghāni Marghīnānī, *Al-Hidāyah* , 3 vols. (Beirut: Dar ahya turas al-arabi, n.d)

[66] Jeanette Wakin. *The Function of documents in Islamic Law* (New York: State University of New York Press, 1972).

[67] Ron Shaham, *The Expert Witness in Islamic Courts: Medicine and Crafts in the service of Law* (London: The University of Chicago Press, 2010).

[68] Shams al-Dīn Abū 'Abd Allāh Muḥammad ibn Abī Bakr ibn Ayyūb al-Zur ī l-Dimashqī l-Ḥanbalī Ibn Qayyim, al-Jaūzīah , *al-Turuq al-Hukmiyyah fi al-Siyasah al-Shar'iyyah* (Cairo: Dār ul-Madni, n.d).

[69] 'Adnān Ḥassan 'Azāīza, *Ḥujjīah al-Qarāi'n fi Sharī'ah al-Islāmiah al-basmāt - al-kiyāfah - dalalāt al-'asar-teḥlīl al-dam (Uman: Dār al-'Amār, 1989).*

books that covers the latest issues in the light of Sharī'ah such as fingerprints, DNA, etc. As the book was published in 1990, it provides basic understanding of the modern means of proof, and does not entail the latest advancement on these issues.

A Ph.d dissertation by a Abūhamid M. Abdul-Quadir, *Shahādah*: the Role of Witnesses in the Islamic Law of Evidence[70], is a compact collection of rules related to the oral testimony in *Ḥanafī Fiqh*. This dissertation discusses conditions of testimony in detail. Another Masters dissertation in Arabic, *Al-Bayīnah fī a-Shar'īah wal-Qānūn*[71], presents a collection of rules regarding *turuq al-Ithbat* (means of proof). The author, Muḥammad Zakrīyah Maḥmood Ṣārī, means of proof in Islamic law in great detail.

A masters level thesis by Muhammad Talal Usli titled as, "Aḥkām Ijrā al-Shahadāt bil-Wasa'l al-Ḥadīsah"[72] is a detailed book on general principles of *Sharī'ah* regarding evidence and *shahādah* (testimony). In this thesis the student has given a detailed introduction of the topic like what are electronic evidences? What are its new types? It has also discussed a few aspects of *Sharī'ah* on electronic evidence. Current thesis lacks discussion on comparison of Islamic law with that of western law. The focus of the study is to highlight the Islamic law on the subject.

An article with the name of "Al Quwah al-Thabūtiah lil-Mu'amalāt al-Ilectroniah"[73] is latest study on electronic laws. It is basically based on Review of the legislative scenario of major Muslim countries like Yemen, Jordan, Palestine, Iraq, Bahrain. This article is a good guide on the legal developments that have taken place after the UNCITRAL conventions on

---

[70] Abuhamid M. Abdul-Quadir titled "*Shahādah*: The role of witnesses in the Islamic law of Evidence," (Ph.D. diss., Utah University, USA, 1997).
[71] Muḥammad Zakrīyah Maḥmood Ṣārī, Al-Bayīnah fī al-Shar'īah wal-Qānūn (Masters diss., Jām'iah Beīrūt, Lebonon, 2006).
[72] Muḥammad Talāl 'Uslī, "Aḥkām Ijrā al-Shahadāt bil-Wasa'l al-Ḥadīsah", (M.S diss., Al Jamiah Islamiah Ghaza, 2011).
[73] Ḥusaīn bin Aḥmād al-Madnī. "Al Quwah al-Thabūtiah lil-Mu'amalāt al-Ilectroniah" Majallah Buḥus al-Qada'ia 7, June (2007), 7-76.

electronic trade and electronic signatures. After these codes given by UNCITRAL model laws, most of the states admitted it impliedly as a parent guide. These recommendations are incorporated in the local laws governed by the states. This article is in Arabic and describes the legislations. The article mainly discusses different implications of electronic transactions in the light of legislations being made by the above-mentioned countries.

An Article titled, "*al-Tijārah electroniah 'Ibr al-Internet Aḥkāmūha wa atharūha fil fiqh al-Islāmi wa nizām al-Sau'di*"[74] by Dr. '*Ali bi 'Abdullah al-Shehri* has written on the same topic. It is basically dealing with Saudi legal system with reference to the electronic laws and legislations. It defines the matters of Meeting of the parties, and other all necessary underlying concepts of electronic trade law. This article is in Arabic and is limited only to Saudi legal system only.

Another article with the topic "Ḥūkūm Ijrā al-'Aqd bil alāt Itīsāl al-Ḥadīsa"[75] by the writer 'Ali Mūhīūdin Qara daghi is a good attempt on this topic. It compares modern electronic laws with that of classical Islamic Law of Shahādāt. Writer cites sources from the classical literature and takes out the similarities and dissimilarities of modern law of electronic evidence and Islamic law of evidence.

Another good article about the electronic law of Jordan is "*Itār al-Qanūnī lil 'Aqd al-Mūbram bil wasae'l Itīsāl al-ḥadīsa*"[76] by *Masūr al-Sararirah* is a good article and revolves around the legislation being made in Jordan. It circulates basically around two important issues. First of them is the matter of Jurisdiction if a dispute arises. Which country's law will prevail in case the dispute arises between different states? Secondly, this article is basically

---

[74] 'Ali bi 'Abdullah al-Shehrī. "al-Tijara electroniah 'Ibr al-Internet Aḥkāmūha wa atharūha fil fiqh al-Islāmi wa nizām al-Sau'di", Majellah al-Būḥūs al-Fiqh al-Mua'sira

[75] 'Ali Mūhīūdin Qara daghi, "Ḥūkūm Ijrā al-'Aqd bil alāt Itīsāl al-Ḥadīsa", Tadrees Ma'had al-Alī, Riyaad (2005), 1-13.

[76] Masūr al-Sararirah, "Itār al-Qanūnī lil 'Aqd al-Mūbram bil wasae'l Itīsāl al-ḥadīsa" Majella Jami'a Damish lil-'Ulum al-Iqtisādiah wal-Qanūn 25, issue no 2 (2009), 1-26.

analysing and comparing Islamic law of contract with that of the Electronic laws of Jordan. This is also the scope of this study. But the study of this article is limited to Jordan only. The scope of this thesis is broader covering from western countries to Muslim countries.

Jamia' 'Umul 'Qura has published on their website the curriculum of crimes committed through latest means so what will the treatment of it. It is a significant and detailed study about the crimes. However, the scope of this study is commercial transaction "Al-Qaza bil Qara'in al-Mu'asira" by Doctor Ibrahim bin Nasir al-Hamooud is a good detailed study on the modern circumstantial evidence and their legal validity to serve as a strong evidence. This article tells about the usage of modern techniques to locate a crime. E.g. DNA test is strong evidence to prove the crime of *Zina*. Similarly, if there is other electronic means available to prove or authenticate, or strengthen the judgement in the favour of one of the party then what would be the result of this type of evidence? It is a good study and focus only on one aspect of the subject i.e. circumstantial evidence. However, the scope of this study is vast. Circumstantial evidence will serve as a part of it.

Apart from above mentioned books, a lot of material can be found on the topic of "evidence", however noteworthy work is missing regarding admissibility of electronic evidence according to *Sharī'ah*. Research will endeavour to focus on *Shari'ah*'s point of view about admissibility of electronic evidence and discuss the issues like what is the legal ground for permissibility of electronic evidences to be presented in the court of law? Whether electronic evidences meet the standard of *ithbāt* in Islamic law of evidence? If yes how? And this research will do a comparison of *Sharī'ah* with some western and Muslim countries.

English law

This section presents a survey of the literature available related to electronic evidence and its related issues. The literature review presented in this section is rather limited, as all the

sources could not be mentioned due to the time and space constraints. However, some of the notable works are mentioned briefly.

A famous scholar in the field of Law and Information Technology, Mason, has edited a book, Electronic Evidence, with the help of a professional team[77]. The book is designed in a way that first seven chapters are dedicated to most of the technical and legal issues related to electronic evidence. The next portion consists of brief introduction of electronic evidence in different countries, such as, Canada, Australia, India, England, USA etc. The authors have tried to discuss majority of the issues related to electronic evidence in detail, which makes the book rather lengthy. Mason and his team's work are the most significant source used for this research. The scope and area of research of the book is rather broad and so can serve as a guiding source as it highlights many good bibliographical researched material sources.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,[78] is another detailed source book, aimed at helping the investigating officers and lawyers to deal with electronic search and seizure. It discusses the different legal issues regarding e-evidence that may arise during a criminal trial. The book primarily focuses on the privacy issues of citizens during an investigation. It mainly deals with privacy laws of USA. [79] The first two chapters contain rules regarding search for evidence with or without warrant. The next two chapters contain the extent of disclosure in the light of existing relevant statutes. The thesis work discusses some of the privacy issues in the second part of

---

[77] Stephen Mason et al., *Electronic Evidence* 2nd edition (Haryana: LexisNexis, 2012).

[78] Orin Kerr, "*Searching and Seizing computer and obtaining electronic evidence in criminal investigations*" *U.S* Department of Justice, Computer Crime and Intellectual Property Section, 2001. http://www.cybercrime.gov/s&smanual2002.htm, October 2004. (accessed September 1, 2015)

[79] Fourth amendments is about protection of privacy of US citizen during investigation. It says the search cannot be conducted without a "Search Warrant" unless in exceptional cases. And that the search must be done only in those items which are mentioned in the Warrant.

third chapter. The four stages of admissibility suggested in this thesis have also been the discussed, but very briefly.

A guide book, Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors[80], identifies and briefly addresses some of the key issues related to digital evidence. It gives a quick glance to search and seizure issues, integrity, discovery, disclosure of digital evidence, courtroom preparation and evidence rules, presentation of digital evidence, and it finally concludes with the discussion of the application of digital evidence on a child pornography case. The guide is essentially based on the "how-to" kind of information. It is designed to create an initial awareness among the investigating officers as well as legal practitioners in order to deal with electronic data. But the books subject matter is not mainly about law, rather it covers the technical issues as well such as chain of custody, integrity etc. As in the field of digital evidence, the technical and legal issues often overlap with each other, a lawyer has to study technical matter and vice versa. Although, the guide is purely based on the US laws, it offers solid guidance to the beginners, and help in gaining a brief introduction of the subject. Procedures are given in clear and uncomplicated manner which can be helpful in making concepts.

Another book Digital Evidence and computer crime: Forensic science, computers and the internet, by Eoghen Casey is a book that explains the concepts in a simplified manner. Book is quite theoretical covering fewer practical examples.

"E-Discovery: current Trends and Cases" by Ralph C. Losely is a book that introduces the modern new field of Information Technology. It is derived from a popular internet blogger of e-discovery, who is a senior attorney at a renowned government law firm. It includes deep,

[80] David W. Hagy, "Digital evidence in the courtroom: a guide for law enforcement and prosecutors." *National Institute of Justice* (2007). https://www.ncjrs.gov/..../211314.pdf (accessed September 1, 2015).

authentic and legal critics and practical opinions. It does not only explain the legal reasoning but it also explains the technologies behind it.

A thesis by the name of "Digital Evidence" written by the name of Muhammad Azhar Ghani deals with the same subject matter. Almost whole of the thesis is explaining the underlying concepts regarding electronic evidence. It briefly explains the concepts and underlying terminologies.

Another Research project named as "critical appraisal of the relevancy and admissibility of electronically generated evidence in Nigeria" by Lawal Ibironke Maryam provides a good deal of preliminary knowledge on the legal scenario of electronic evidence of Nigeria. It also tells the latest advancements being made in Nigeria and suggests changes in the legal structure. The good thing about it is that it also gives a brief introduction of general law of evidence.

The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime-Results of a European Study[81] is a project conducted by Cebex intelligence on e-evidence. The project report focuses on the problems faced by the European Social Agents involved in collecting, analysing and presenting electronic evidence and their actual operations. The project team also conducted a survey, which shows statistic data collected in almost 25-30 European countries. It discusses the main hurdles faced while dealing with the e-evidence. It includes surveys taken from different judges and legal professionals regarding the problems they face while dealing with technical evidence. The major problem highlighted as a result of the survey was lack of awareness.

[81]Fredesvinda Insa , "The Admissibility Of Electronic Evidence In Court (A.E.E.C): Fighting Against High-Tech Crime-Result of a European Study", *Journal of Digital Forensic Practice*. 1, no. 4, (2007), 285-289, http://dx.doi.ord/10.1080/155 67280701418049. (accessed May 9, 2017).

Digital Evidence and the U.S. Criminal Justice System, Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence[82] by Goodison, Davis, and Jackson, discusses the rise of digital evidence, unique challenges, and the results of a workshop held to prioritize needs in digital evidence processing. The report highlights new emerging issues regarding the modern cell phones and discusses the forthcoming problems that the law enforcement agencies may face, after Apple Corporation's decision to not disclose private information of any citizen even at the request of police officer. The article contributes research in the field of electronic evidence in a criminal trial.

A Journal, Obtaining and Admitting Electronic Evidence[83], consists of six articles dealing with different issues. The first of them is, Using Log Record Analysis to Show Internet and Computer Activity in Criminal Cases by Mark L. Krotoski[84] and Jason Pass Water. This article mainly deals with the key role of log records in a criminal investigation or trial and evidence collection. As a matter of fact, log records play a key role in solving most of the criminal cases and investigations. The remaining articles from the journal serve as useful guides and a source for procedural regulations.

There are a large number articles that cover the area of computer evidence. Developed legal systems proceed swiftly in absorbing the new computer technologies in their existing legal systems. A few of the articles related to computer evidence are mentioned below. The rest of the articles shall be cited wherever quoted in the thesis.

---

[82]Goodison, Sean E., Robert C. Davis and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System.

[83]Mark L., Krotoski, et all "Obtaining and Admitting Electronic Evidence." *United States Attorney's Bulletin* (2011).

[84] Ibid.

An article titled, Discovery, Evidence, Confidentiality, and Security Problems Associated with the Use of Computer Based Litigation Support Systems[85] by Fromholz, serves as a good learning source. It focuses on the problems of admissibility of computerized records in general, and the issues of admissibility, confidentiality, and security in particular. The author mainly focuses on the hearsay and original writing rule. Fromholz is of the opinion that there is no need to alter the basic rules of evidence, discovery, or confidentiality while dealing with electronic evidence. According to Fromholz, even though the electronic evidence is very different in nature but it can still be dealt under the ordinary law of evidence in a very effective manner. Fromholz states that the suggestion pertaining to issuance of a separate law that deals with electronic evidence only, should be overlooked and electronic evidence should be tried under the existing law. It will not only save time and energy, but will also be easier for the community at large to absorb and understand.

Another article, The Discovery and Use of Computerized Information: An Examination of Current Approaches by Long, [86] focusses on the issues of discovery of electronic evidence. The author has broadly categorized the article into two parts. The first part deals with the issues of discovery of electronic information. The second part focusses on the evidential problems of reliability of computer-generated evidence. The article though brief, is highly significant piece of research. Long emphasizes on the training of the legal practitioners and judges to deal with these issues of electronic evidence. Long further stresses on and acknowledges how effectively the electronic evidences are dealt under the existing laws of evidence and recommends that it is the right course to proceed on.

---

[85]Haley J. Fromholz, "Discovery, Evidence, Confidentiality, and Security Problems Associated with the Use of Computer-Based Litigation Support Systems", *Wash. U. L. Q.* (1977): 445 http://openscholarship.wustl.edu/law_lawreview/vol1977/iss3/10.

[86] Richard M. Long, "The Discovery and Use of Computerized Information: An Examination of Current Approaches", *Pepp. L. Rev.* 13, no. 2 (1986) http://digitalcommons.pepperdine.edu/plr/vol13/iss2/6

Another article, Digital Data as Hearsay by Teppler,[87] examines the proposition that all the digital data is hearsay. The article addresses the issue of inadequacy of approaches to deal with hearsay exceptions used to offer computer generated evidence. It was suggested that if hearsay exception is not sought, it should be considered as hearsay. And if the evidence is admitted on the basis of hearsay exception, it should be subjected to heightened reliability requirements.

Law of Evidence in Canada: the Uniform Evidence Act, Twelve Years Later[88] is another significant research article by Duranti, Rogers and Sheppard. It examines the adequacy of the law after 12 years. The authors believe that in view the complicated nature of electronic evidence, minor changes in the existing law are not adequate. The authors suggest that there should be a new set of laws to deal with electronic records.

An article, When the not-so- Wild things are Computer in the Courtroom, Federal rule of Evidence and the Need for Institutional Reforms and more Judicial Acceptance[89] emphasizes on the use and admissibility of Computer-Generated Exhibits (CGE). The author states that pictures have always served as a good source of understanding for the judges and proposes that ever more computer technology should be introduced in the court room so that the system of justice becomes efficient.

An article Are Your Eyes Deceiving You?, the Evidentiary Crises Regarding the Admissibility of Computer Generated Evidence[90] by Fielder discusses the Computer

---

[87] Stephen Teppler "Digital Data as Hearsay", *Digital Evidence and Electronic Signature Law Review* 6, http://sas-space.sas.ac.uk/5334/1/1853-2571-1-SM.pdf (accessed September 1, 2015).

[88] Luciana Duranti, Corinne Rogers and Anthony Sheppard, "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", *Arhivaria*70 (Fall 2010): 95-124.

[89] Fred Galves, "When the not-so- Wild things are Computer in the Courtroom, Federal rule of Evidence and the Need for Institutional Reforms and more Judicial Acceptance", *Harvard Journal of Law & Technology* 2, no. 13 (2000); 165-300.

[90] Betsy s. Fiedler, "Are your eyes deceiving you?: The evidentiary crisis regarding the admissibility of computer generated evidence" *NYL. Sch. L. Rev. 48* (2003): 295.

Generated Evidence. It focuses on the use of animations and simulations and discusses the evidentiary standards of both.

Similarly, the article, Admissibility of Electronically Stored Information: It's Still the Same Old Story[91] by Finkelstein and Storch, discusses the evidential standards of admissibility which includes, relevance, authenticity, hearsay and original writing rule. The authors are of the view that even though electronic evidence does not completely constitute the investigation of a trial but it constitutes a significant portion of it.

Another article, Admissibility of E-Evidence under the Federal Rules of Evidence[92] by Freider and Murray, presents an overview of "how to get it right on the first try". It is roughly organized with examples on how to apply the evidential rules on electronic evidence from the perspective of Federal rules of Evidence of USA.

A research paper with the title "Admissibility of non-U.S. Electronic Evidence" by Kenneth Rashbaum, Matthew F. Knouff, and Dominique Murray is a rich report written on the preliminary criterias of laws that the court talk about in the first instance when the electronic evidences are presented before them. The report does not cater the upcoming and latest issues and status of electronic evidences.

---

[91] Sheldon M., Finkelstein, and R. Storch. Evelyn. "Admissibility of Electronically Stored Information: It's Still the Same Old Story." *J. Am. Acad. Matrimonial Law*. 23 (2010) www.aaml.org/sites/default/files/MAT101_2.pdf (accessed: September 1, 2015).

[92] Jonathan D. Freider and Leigh M. Murray. "Admissibility of E-Evidence under the Federal Rules of Evidence" *Rich.J.L. & Tech 17*. no.2 (2011). http://jolt.richmond.edu/17i2/article5.pdf.

Pakistani law

A renowned cyber lawyer of Pakistan has compiled a number of books on digital evidence. One of them is "Digital Evidence, Forensic laws &CCTV camera". [93] The book discusses different judgements on electronic evidence. It discusses regarding admissibility of different form of evidence like CCTV camera. But it does not give a comparison to Islamic and western law.

Another book of the same writer is "New Cyber Law in Pakistan"[94] this book addresses recent legislation Prevention of Electronic Crimes Act 2016. It serves as a commentary to this law. It discusses the theory, practice and case laws. But this book does not discuss the rules of admissibility for electronic evidence, nor cyber laws other than discussed in PECA 2016.

Another article on "privacy and Islam" [95] discusses status of privacy in Islamic law and its application on Data protection laws of Pakistan.

Justice (R) Khalil-ur-Rehman Khan presented a paper in International judicial conference, titled "Cyber Laws In Pakistan", [96] published by supreme court is an article written on the basic notes of cyber laws of Pakistan.

The above literature review shows that issues of electronic evidence are very well addressed from all aspects in western law. As there are large number of books, articles, documentaries and reports present on the subject. But the case is different in Islamic and Pakistani law. In Islamic law the material available is mostly confined to the status of permissible and impermissible. The research is in formative stage. This area needs special

---

[93] Shahid Jamal Tubrazy, Digital Evidence forensic laws and cctv camera (Lahore: Key law reporter publication, 2018)

[94] Shahid Jamal Tubrazy, New Cyber laws in Pakistan, (Lahore; Key law reporter publication, 2017)

[95] Muhammad Aslam Hayat (2007) Privacy and Islam: From the Quran to data protection in Pakistan, Information & Communications Technology Law, 16:2, 137-148

[96] Khalil-ur-Rehman Khan, "Cyber Laws In Pakistan" http://www.supremecourt.gov.pk/ijc/articles/10/1.pdf

attention of Islamic scholars. Current thesis will try to dig out principle analysing Islamic law in a deeper manner.

It is also evident from the above literature review that none of the researches mentioned above are comparing western, Islamic and Pakistani law all together. In researches of western and Islamic laws, ample discussion regarding analysis of national legislations of different countries is present. But it is not in the knowledge of the author if anyone has compared the basic theories of Islamic and western law of evidence and applied them on Pakistani law. The aim of this thesis is to analyse western law from the perspective of Islamic law and suggest changes for Pakistan law of electronic evidence.

PART 1

CHAPTER 2 ELECTRONIC EVIDENCE IN ISLAMIC LAW

2.1 Electronic Evidence

Fourteen hundred years ago, Islam introduced a very compact yet universally applicable legal system. It contained all the elements and essentials of a legal system, the effectiveness of which is still being discovered in today's world. There is no legal aspect that is not covered by the Islamic law. It has no loop holes and lacunas, other than the misinterpretations made by the ill-prepared scholars.

Islamic legal system has introduced principles of evidence, which in comparison with today's legal systems, are much more elaborative. The main purpose of this chapter is to derive principles of e-evidence. Alongside the principles, the existing of evidence in Islam is also discussed, as the topic is closely related to e-evidence.

There is ample discussion present in literature regarding the rules of physical evidence in Islamic law. But as e-evidence came into existence only in the recent past, the electronic evidence is not directly addressed in the classical jurisprudence. Islamic law does not provide rules for electronic evidence, but it does provide important general principles, especially in the area of documentary evidence and expert testimony, that can be used to test the standards advocated by modern law with a view of ascertaining compatibility.

An analysis of Islamic law of evidence is essential to have a general understanding of Islamic courts. This chapter will discuss in detail the general principles of Islamic law of evidence. The chapter will elaborate the seven means of proof in Islamic law. With special focus on the four means of proofs which are closely related to electronic evidence. The four means are the oral testimony, circumstantial evidence, expert testimony and documentary evidence.

Evidence is a general term, which includes different means of proof. In Islamic law there are seven means of proofs. All of them cover details of Islamic law of evidence. While

on the other hand, English law also has different means of proofs, which are almost similar to Islamic law. For instance, in English law, authentication by circumstantial evidence, testimony, expert witness and documentary evidence, etc., these modes of authentication are exactly the same as in Islamic law. [97]

The section of Oral testimony (*Shahādah*) will provide an overview of how the law of evidence works in the Islamic legal system. Documentary evidence shall be discussed at length because it explains the legal worth of documentary evidence in Islamic Law. This will lead us to have an idea of legal worth of e-evidence because electronic evidence is documentary evidence.[98] Expert testimony and circumstantial evidence are quite important in Islamic law. They have a complete set of precedents in books of classical Islamic law. Thus, making it easier for the law students to derive the validity of modern means of proofs in Islamic law.

2.2 General Principles of Evidence

The judge has a central role in judicial proceedings whose responsibility is to establish both the right of Allah (public rights) and the rights of man (Private right) to settle disputes by attaining competent evidence. There are three ways for the judge to acquire knowledge;

1. By confession
2. By oath
3. By evidence

[97] See chap 3, para 3.4.5.
[98] As it was held in High Court of Karachi in *Sikandar Ali Lashari v. The state* 2016 YLE 62 Karachi-High_court-Sindh, that a CD or USB on a computer and other electronic evidence are documentary evidence.

The matter can be resolved speedily if the accused confess the facts. If the accused does not confess, then the plaintiff is supposed to produce evidence. In case the plaintiff fails to produce evidence, the defendant shall be required to take an oath in favour of denial. [99]

Oral testimony (*Shahādah*) is a major type of evidence in Shar'īah. Other evidences include written documents, circumstantial evidence and scientific evidence. There is a famous saying of the Prophet (PBUH) that the evidence must be produced by the plaintiff and oath must be made by the defendant.[100]

The word used for Evidence in Arabic is "*bayīnah*". The literal meaning of this term is "visible or glowing". It is derived from the word "tibyān" which means an act of explaining and showing how something works or is done or emphasizing; publishing; making evident. It means visible or strong evidence.[101]

Technically, it denotes the strong argument, evidence or a strong proof. The technical definition of this word is *bayīnah* is well defined by *Ibn Qayyim*[102]:

> He says, "Evidence (al- *bayīnah*) as an umbrella term stands for all that, what manifests the truth and disclose it. Anyone who restricts it to two eyewitnesses or of them or one of such witnesses does not do justice to the true signification of the term. The holy Qur'ān never uses the word *bayīnah* to mean two witnesses alone. The Qur'ānic connotations of the word *bayīnah* therefore are *ḥujjah* (proof), *dalīl* (evidence), and *burhān* (clear proof)."[103]

---

[99] Prophet (PBUH) said, "Evidence must be produced by the plaintiff and Oath must be made by the defendant"Kasani, Vol 7/287

[100] 'Alā' *al-Dī*n Abu Bakr bin Mas'ud bin 'Aḥmad al-Kāsānī. *Badā'i' al-Ṣanā'i fi tart īb al-sharā'i*. 2nd ed. vol. 7 (Dār al-Kutub al-'Ilmīah,1998), 287.

[101] Al-Mu'jam al-wasīt, s.v "Bayīnah" dar al-arabi, 1/80.

[102] *Ibn Qayyim al-Jawziyya* (1292–1350 CE / 691 AH–751 AH), whose full name was, *Shams al-Dīn Abū 'Abd A'llāh Muhammad ibn Ahī Bakr ibn Ayyūb al-Zur ī l-Dimashqī l-Ḥanbalī* . He was born on 7 Safar 691/29 January 1292 in Damascus. He wrote many books among which are, *Zād al-Ma'ād, Rawḍat al-Muḥibbīn, and Badā'i' al-Fawā'id.* He died in 1350 at the age of sixty.

[103] Shams al-Dīn Abū 'Abd Allāh Muḥammad ibn Abī Bakr ibn Ayyūb al-Zur ī l-Dimashqī l-Ḥanbalī Ibn Qayyim, al-Jaūzīah , *al-Turuq al-Hukmiyyah fi al-Siyasah al-Shar'iyyah* (Cairo: Dār ul-Madni, n.d), 13. Translated by Sayed Sikanadar Shah Haneef, Modern Means of Proof: Legal Basis for Its Accommodation in Islamic law, Arab Law Quarterly, Vol. 20, No. 4 (2006), 346.
(Accessed last 24rth March, 2017) http://www.jstor.org/stable/27650561

According to *'Ibn Taīmīyah*[104] and *'Ibn Qayyīm, this* word connotes the meaning such as: testimony, strong circumstantial evidence (*qarā'in qāṭ'iah*), documentary evidence and expert testimony. On the contrary *Ḥanafī* jurists think that that word *bayīnah* and *Shahādah* are not similar in meaning. *Bayīnah,* according to them, is a general term which denotes all the clear and conclusive evidences which are helpful to prove any fact in issue. In other words, the term *bayīnah* is general (*'ām*) and term *Shādah* is specific (*khāṣ*) and it denotes testimony only.[105] So, the term *bayīnah* includes all the means of proofs. There is a misconception that Islamic law of evidence is confined to testimony only. It is not true. The Islamic law of evidence constitutes of all the means of proofs which are discussed at length by the worthy jurists. This makes the Islamic law flexible enough to absorb the upcoming changes in the society resulting from high-tech environment.

2.3 Means of Proof

Under Islamic law of evidence, a fact can be proven before court in seven ways;

1. Al-Yamīn (Oath)

2. Al-Iqrār (admission/confession)

3. Al-*Shahādah* (testimony)

4. Al-Kitābah (documentary evidence)

5. Ra'yu al-khabīr (expert opinion)

---

[104] *Ibn Taymiyyah*, in full *Taqī al-Dīn Abū al-'Abbās Aḥmad ibn 'Abd al-Salām ibn 'Abd Allāh ibn Muḥammad ibn Taymiyyah*. He was born in 1263 in Harran. He died in September 26, 1328 in Damascus). Ibn Taymiyyah wrote a large number of books; he wrote more than three hundred books the most famous of them are kitāb al 'Imān, minhāj al-Sunnah al-nabwīah, al-'aqidah al-waītah etc.

[105] Justice Tanzil-ur-Rehman, *Islamī' Qanūn-e-Shahadat* (Lahore: Pakistan Educational Press, 1988), 37.

6. Al-*Qarīna* (circumstantial evidence)

7. 'Ilm al Qāḍī (knowledge of a judge) [106]

It is worth mentioning here that similar kinds of proofs are mentioned under the English legal system, other than Oath and 'Ilm al Qāḍī (knowledge of a judge), as modes of authentication for physical as well as electronic evidence. There is not much difference in the law of evidence in English law and Sharī'ah law. Both the legal systems require that the evidence must be reliable, authentic, and must not be hearsay.[107]

Means of proof are also of great importance from the perspective of electronic evidence in Islamic law. These means are especially helpful in proving or disproving electronic evidence.

2.3.1 Al-Yamīn

Al yamīn, a mean of proof, means "the right side" in the literal sense it also means "oath". A person who takes an oath usually does so by putting up his right hand. It also known as "al-ḥalaf", al-istiḥlāf" and al-qasam". [108]

In the technical sense, an oath is an utterance accompanied by the invocation of Allah's name for purposefully stating by way of oath. Oath is defined as the purposive stating of an improbable matter and strengthening the statement by invoking the name of Allah Almighty or by invoking one of his Attributes.[109] Oath is also a purposive way of making a statement over a probable matter or improbable matter coupled with the invocation of the name of Allah

---

[106] Wahbah al-Zuhaīlī, *"al-Fiqh al-Islamī wa 'Adiltuhu" vol. 6 (Damascus: Dār al-fikr, 1985). 555.*
[107] See Chap 3, para 3.1 and 3.2
[108] *Maūsūa Fiqhiyah al-Qūītīyah.* s.v *"al-Yamīn"*.
[109] Al-Misbaḥ al Munīr fī Gharīb al-Sharḥ al-Kabīr. s.v "Al-Yamīn" vol.2/681

Almighty or His Attributes. It is also used to strengthen or to clarify a matter and help mitigate ambiguities. For example, saying "Wallahi" and invoking the Attributes of Allah such as "Al-Raḥmān" and "Al-Raḥīm". There are various evidences from the Qur'ān and *Sunnah*, which proves that the oath is an acceptable mean of proof. Allah Almighty says:

لَا يُؤَاخِذُكُمُ ٱللَّهُ بِٱللَّغْوِ فِىٓ أَيْمَـٰنِكُمْ

وَلَـٰكِن يُؤَاخِذُكُم بِمَا عَقَّدتُّمُ ٱلْأَيْمَـٰنَ[110]

"Allah will not impose blame upon you for what is meaning less in your oath".

Here in *Qur'an*, Allah the Exalted quotes this verse in order to explain that the oath taken during communication without intention of taking oath does not bind a person. This automatically implies that oaths taken with intention of swearing upon Allah Almighty, binds a person making it. A person who breaks it is liable to pay certain amount of money prescribed by *Qur'an*, which is known as Kafārah.[111]

Similarly, in courts facts are proved and disproved on the basis of oath. This fact is further authenticated by a number of traditions of Holy Prophet (PBUH). For instance, there is a tradition of Holy Prophet (PBUH) about the legal validity of Oath:

عَنْ وَائِلِ بْنِ حُجْرٍ رَضِيَ اللَّهُ تَعَالَى عَنْهُ - أَنَّ النَّبِيَّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ لَهُ: شَاهِدَاكَ أَوْ يَمِينُهُ

[110] Al-*Qur'an* [5:89]
[111] Muḥammad bin Jarīr al-Ṭabri, Jāmay' al-Bayān fī Ta'wīl al-Qur'an, vol. 23 (Beirut: Mūasasah- ur Risālah, 2000), 523.

It was narrated by Companion of Prophet (PBUH) *Wa'il ibn Ḥujr that the* Prophet (PBUH) said, "Produce your two witnesses or else the defendant is to take an oath" [112]

Another very famous tradition of Prophet PBUH on this subject matter is:

"البينة على المدعي واليمين على من أنكر"

"Evidence must be produced by the plaintiff and Oath must be made by the defendant".[113]

Traditions of Prophet (PBUH) are clearly implying that plaintiff is bound to present testimony and evidence and if he fails to do that, the defendant swears upon Allah Almighty about proving or disproving of a fact. [114]

2.3.2 Al-Iqrār

Al-Iqrār is a mean of proof of evidence which literally means confession or admission. However, the meaning of this term can be classified into two definitions; the Shāf'ī and the *Ḥanafī* definition. Shāfī defined al-Iqrār as a;

"Testimony of the existence of a proved right against the maker of the admission himself."[115]

It also defined as recognition (al-'A'tirāf). While, the *Ḥanafī*'s definition al-Iqrār is an

"Admission of the existence of the right of another person against the maker of the admission himself."[116]

---

[112] Muslim bin al Ḥjāj Abū al-Ḥassan al-Qashīrī al-nīsābūrī, *Saḥīḥ Muslim,* (Beīrūt: dār 'Iḥyīā' al-'arabī. n.d), Vol.1/123. Tradition no. 221

[113] Kasani, vol.7, 287.

Muḥammad bin Maḥmūd al Bābarti, *Al Anāyah Sharḥ al-Hidāyah*, vol. 8 (Dār al Fikar: n.d), 153. Also, in [114] Abū Ḥassan Nisābūrī, Al Wasīt fi Tafsīr al-Qur'an al Majīd, vol. 3 (Beirut: Dār al Kitāb, 1994), 545.

[115] Muḥammad Zakrīyah Maḥmood Ṣārī, Al-bayīnah fi al-Shar'īah wal-Qānūn (Masters diss., Jām'iah Beīrūt, Lebanon, 2006), 164.

[116] Ibid.

It also means testimony of the existence of right or interest (thabāt al-ḥaq) for the benefit of another person and detrimental to the right or interest of the maker of the admission himself through the use of specific wordings.

Al-Iqrār also means a statement, oral, documentary or using gestures, made by a person meaning to show that he is under some obligation to another person in respect of some right.[117]

The admission has three types or instances;

1. Oral confession

2. Admission made by signs that given by a person who is dumb

3. Written admission that is made using ordinary paper, [118]

Confession (Iqrar) is an oath which is a statement, (oral, written or using gestures) made by a person that he is under an obligation to another person in respect of some right of that person against him and which is raised by any person under any of the circumstances mentioned hereinafter. It is, therefore, a specific admission or acknowledgement as a mean of proof to indicate a right or interest of another against oneself, or to admit to an offence or liability against oneself.[119]

Admission or confession made through electronic means is admissible. For example, an instance of a plaintiff who has admitted to certain facts in an email or a text message, which are undoubtedly proved to be his. They are a strong admissible evidence. If that evidence can be corroborated or authenticated by other evidence, it can help in convicting the criminal.

---

[117] *Maūsūa Fiqhiyah al-Qūītīyah*, s.v "*Al-Iqrār*".
[118] See Qanun-e-Shahadat Order §30 "Admissions"
[119] Najah Abdulaziz. "The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia," (Ph.D diss., Demonfort University, UK, 2015), 105.

2.3.3 Shahādāh – Oral Testimony

The third mean of proof in Islamic law is the oral testimony (*Shahādah*) which is equally important in the western legal systems. It plays an important role in proving facts before the court. When someone is accused of a crime and he denies it, the burden of proof lies on the plaintiff. Thus, the judge asks the plaintiff to bring his witnesses or any other evidence to support his claim.[120]

General rules of testimony in Islamic law are discussed in the books of *fiqh,* under "*kitāb-al-shahādāt*". These fiqh books have categorized this topic under the following headings; rules of admissibility of testimony, conditions for the admissibility of testimony; the reasons of rejection of testimony; disagreement of witnesses in their testimony, etc.

This chapter covers the topic of testimony by giving an overview on its definitions, legal validity of *Shahādah* from Qur'ān, legal force of *shahādah* in *Sunnah*, elements of *shahādah* ('Arkān al- *shahādah*), its categories, conditions, grounds of rejection, women's testimony, purgation of witnesses, hearsay rule, secondary witnesses and finally a comparison between the Islamic and English concepts of testimony.

2.3.3.1 Definitions

This section provides an overview of the literal definition of *shahādah*, its definition according to the different jurists and lastly the intended definition.

2.3.3.1.1 Literal Meaning of Shahādah

Shahādah literally denotes to a diverse set of meanings such as'knowledge, attendance, and an act of informing'. If it is used in the past tense, the equivalent verb is *shahida* [شهد],

[120] Prophet PBUH says "Produce your two witnesses or else the defendant is to take an Oath" Kāsāni, vol.7, 287.

which means 'to attend or witness something'. The basis of testimony about any incident or event is direct observation or inspection. Similarly, a *shāhid* [شاهد] is a noun who is a well-informed person explaining what he has inspected or knows about a particular incident or some other thing of which he has personal knowledge. While the word *mushāhadah* مشاهده means 'witnessing and observing'. [121]

Testimony in court is dealt as a religious duty.[122] It is an important obligation upon all Muslims. Messenger of Allah (PBUH) is reported to have said:

"Should I not tell you of the best witnesses? They are the ones who produce their evidence before they are asked for it" [123]

Quran states that witness cannot refuse to give testimony once they are demanded. In Islamic law, it is a sin to conceal facts in front of the court. The reason behind it is that it affects the rights of mankind. A verse of *Qura'n* regarding this matter is;

وَلَا تَكْتُمُوا الشَّهَادَةَ ۚ وَمَن يَكْتُمْهَا فَإِنَّهُ ءَاثِمٌ قَلْبُهُ 124

"And do not conceal testimony, for whoever conceals it - his heart is indeed sinful"

This verse denotes that *shahādah* is a religious duty and it must be treated as Amānah. Returning of Amānah is obligatory on a Muslim.

2.3.3.1.2 Meaning of Shahādah According to Different Jurists

***Ḥanafī* Definition**

---

[121] Lisān al-'Arab s.v "***shahādah***".
[122] Burhān al-din abu al-Ḥassan 'Ali ibn abī bakr farghāni Marghīnānī. *Al-Hidāyah* , vol. 3 (Beirut: Dar ahya turas al-arabi, n.d), 116.
[123] Reported by Muslim in his Saheeh, Book of Judgments, hadeeth no. 4494; and at Tirmidhee in his Al-jaami', Book of Testimonies, hadeeth no. 2295.)
[124] Al- *Qur'an* 2:283

Ḥanafī jurists define *shahādah* as, "Informing about something which the witnesses have actually witnessed, be it an act they have seen with their own eyes such as murder or adultery, or something they have heard such as contracts and statements". [125]

Mālikī Definition

The *Mālikī* jurists define it as a statement which requires the judge to issue a judgement on condition that such a statement has been made by more than one just person or following the taking of an oath of the person requesting it. [126]

Shāf'ī Definition

The Shāf'ī jurists define *shahādah* as informing about somebody's right against another person by using specific words. [127]

Ḥanbalī Definition

The Ḥanbalī jurists define the term *shahādah* as the information the witness gives using specific words, such as [أشهد] 'I bear witness' and 'I testify'.[128]

2.3.3.1.3 ***Intended Definition***

Taking into consideration the above definitions the most appropriate definitions of *shahādah* is;

"Giving information by a just witness, with knowledge, regarding the right of a person against another person in a court of justice using specific words".[129]

---

[125] Zaīn al-Dīn bin Ibrahīm bin Muḥammd Ibn Nujaīm, "*al-Baḥr ar Rā'iq Sharḥ Kanz al-Daqaiq*", vol. 7 (Dār al-Kitāb al-Islāmī, n.d), 61. Majallah al- A ḥkām al- 'Adalīayah, rule number 1684. Also in Muḥammad Zakrīyah, "Al-bayīnah fi al-Shar'īah wal-Qānūn", 60. Definition translated by Saleem Marsoof, "Witness Testimony – Some Perspectives From Sharia'at Law Justice" https://www.academia.edu/5466591/Witness_Testimony_Some_Perspectives_From_Shariaat_Law

[126] Muḥammad Zakrīyah, *"Al-bayīnah fi al-Shar'īah wal-Qānūn"*, 60.

[127] Ibid.

[128] Mansūr al-Bahūtī, *Sharḥ Muntahaa al-'Iraadaat*,1st ed. Vol. 3, (Beirut : 'Alam al-Kutub publishers, 1993), 575.

Here, the words 'giving information' includes all types of information, and the word 'just' qualifies the witness, and excludes a person whose testimony is not admissible. The expression 'with knowledge' implies that the witness has to have knowledge about the incident about which he gives testimony.

It doesn't matter if the information given pertains to electronic data. The witness must have personal knowledge or expert knowledge about it. Such evidence is admissible in the Islamic Law. There is no restriction in the definitions regarding the existence necessarily being physical. So electronic evidence can be presented.

2.3.3.2 Dalil of Shahādah from Qur'ān

Testimony has received its legal force from a number of verses from Qur'ān. Allah Almighty has obligated testimony. Qurān has stipulated about the obligation of *shahādah* at many places. One of those verses is:

وَلَا تَكْتُمُوا الشَّهَادَةَ[130]

"And do not conceal testimony"

As stated earlier that testimony is considered as a religious obligation. It is considered as a sacred trust bestowed upon Muslims to bear as witness wherever it is necessary. Muslims are commanded not to conceal the testimony.

Similarly, a verse of the Qur'ān states about the criteria of witnesses. The Qur'ān says that the witnesses must be "just" and "probable":

---

[129] 'Abdur Rehman bin Muhammad al-Mad'u, *Majma' al-Anhur Fī Sharḥ Multaqa al-Abḥur*, vol.2 (Dar 'Iḥya al-turāth al-'Arabi, n.d. 185.
[130] Al- *Qur'an* 2:283

وَأَشْهِدُوا ذَوَىْ عَدْلٍ مِّنكُمْ[131]

"And bring to witness two just men from among you and establish the testimony"

The only reason for demanding just witness is to acquire authentic and reliable evidence. Testimony is reliable only if it is born by a just witness. Though the criteria of a "just witness" has varied from time to time.[132]

2.3.3.3 Legal Force of Shahādah in Sunnah

Sunnah of the Prophet (PBUH) also affirms the legal validity. There are a large number of traditions of Prophet (PBUH) pertaining to the matters of *shahādah*. For instance, the tradition of Wa'il ibn Ḥujr which states that;

وَائِل بْنِ حُجْر رَضِيَ اللهُ تَعَالَى عَنْهُ - أَنَّ النَّبِيَّ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ قَالَ لَهُ: شَاهِدَاكَ أَوْ يَمِينُهُ

It was narrated by Companion of Prophet (PBUH) Wa'il ibn Ḥujr that the Propht (PBUH)

"Produce your two witnesses or else the defendant is to take an oath" [133]

Shahādah is also approved by 'Ijma. The method of oral testimony was adopted by the righteous caliph after Prophet (PBUH). It is '*Ijma* (Consensus) of the caliphs and the Muslim Scholars that *Shahādah* is one of the most important proof of evidence.

2.3.3.4 Elements of *Shahādah* ('Arkān al- *shahādah*)

Elements of *shahādah* (arkan al-*Shahādah*) is a matter in which there is a difference of opinion among the scholars. *Ḥanafī* jurists are of the view that there is only one element of

---

[131] Al- Qur'ān [65:2]

[132] In the beginning the crierias of just witness was strict which became less strict due to change in environment.

[133] Muslim bin al Ḥjāj Abū al-Ḥassan al-Qashīrī al-nīsābūrī. *Saḥīḥ Muslim.* (Beīrūt: dār 'Iḥyīā' al-'arabī. n.d), Vol.1/123. Tradition no. 221

shahādah. It is, the word "I testify" ('Ashhadu). They are of the view that it is the only element of *shahādah* because Qur'ān demanded it. It is observed that, if a person testifies in the past then it is incorrect. For instance, if he uses the words Shahidtu (I inspected or testified), then it is inadmissible. The past tells us about what has already taken place and testimony is to give information about present.[134]

Shāfi'ī scholars, on the other hand have a different opinion on this matter. They say that there are five elements of *Shahādah*, which are;

1. Witnesses شاهد
2. Plaintiff الْمَشْهُودُ لَه
3. Defendant الْمَشْهُودُ عَلَيْه
4. Subject matter of *Shahādah* الْمَشْهُودُ بِهِ
5. Text or wording of *Shahādah* الصِّيغَة [135]

All these five essential elements together make a testimony valid according to Shāfi'ī Scholars. *Ḥanafī*s say that only the word "I testify" is the basis of valid testimony. [136]

There are a number of differences between testimony in English law and Islamic law. The major difference among them is that Islamic law classifies testimony into different types. These classifications are based on the different types of crimes. For instance, Ḥudūd crimes and retaliation have requirement of four and two witnesses simultaneously. Testimony in financial matters, on the other hand requires two witnesses. [137]

---

[134] 'Alā' *al-Dī*n Abu Bakr bin Mas'ud bin 'Aḥmad al-Kāsānī. (d. 587H). *"Badā'i' al-Ṣanā'i fī tart īb al-sharā'ī"*, (Dār al-Kutub al-'Ilmīah,) 2nd ed 1998. vol.6, 266. Also in 'Abdul mughnī bin Ṭalib bin Ḥamād bin 'Ibrahīm al-Damishqi. *"Albāb fī sharḥ al-kitāb"*. vol.4 (Beīrūt: Maktabah 'Ilmiah, n.d) 59. Also, in Wahbah al-Zuhaīlī, *"al-Fiqh al-Islamī wa 'Adiltuhu" vol6. (Damascus: Dār al-fikr, 1985), 556.*

[135] *Fiqhiyah al-Qūītīyah, s.v* " 'Arkān al-*Shahādah*"

[136] Ibid

[137] See Chap. 2 Para 2.3.3.5

Unlike common law, Islamic law also differentiates between testimony of a man and a woman. In fact, Islamic laws frees women from a huge responsibility of testimony in matters related to Ḥudūd and Qiṣāṣ. In financial matters her testimony is acceptable where she would be accompanied by another woman who can remind her in the cases where she forgets.[138]

2.3.3.5 Categories of Shahādah

There are different classifications of testimonies. Islamic Law deals with different crimes requiring different number of witnesses for each. For instance, some Hudud crimes require four witnesses and some require two. Similar is the case with other crimes.

Marghīnānī states in his book that there are two broad categories of testimony in Islamic law; [139]

1. Testimony in the matters related to right of Allah Almighty
2. Testimony in the matters related to right of man

Numerical strength of witnesses varies in both the above cases. In fact, it is fixed by the Qur'ān on case to case basis. In cases of testimony for ḥudūd offences, right of Allah Almighty is involved. While in the matters related to private rights and financial matters, right of man in involved. [140]

In cases of Ḥudūd, the rules of testimony are more stringent. Women are specifically excluded from being witness in these cases. Nevertheless, in cases of hudūd and qiṣaṣ,

[138] Al-*Qur'an* [2:282]. There was a huge criticism by the western society on Islamic law that they are biased towards equality of women. This opinion is neglected by the fact that Islamic law also accepts testimony f single women in the matters where testimony of men is not possible or is very rare e.g matters related to gynecology, first cry of a child or testimony regarding private parts of women etc. In financial matters accompanying her with another women is due to the reason that financial markets where financial markets where financial issues generally grow are not her field. Presence of women in lower in such places as compared to males.

[139] The Hidayah or Guide: A commentary on the Mussalman Laws, Trans. Charles Hamilton, vol. 3 (London: T. Benslay, n.d), 116.

[140] Ibid

witnesses are at liberty either to give or refrain from giving testimony. Rather in these cases it is preferable to conceal the testimony.[141] Prophet (PBUH) said to a person who had borne testimony "Verily it would have been better for you, if you had concealed it".[142] But this rule does not apply in the case of theft where it is not encouraged to conceal the testimony. Rather it is an obligation to give testimony. The reason of excluding theft from this rule principle is that otherwise the right of proprietor will be compromised which is against the rules of justice.[143]

Discussing the rationale of preference to conceal testimony in case of Ḥudūd and Qiṣāṣ, *Marghīnāni* says that it protects from two harms; first is, defamation of character of offender and secondly the *ḥadd* punishment itself.[144]

Witness in Ḥudūd and Qiṣaṣ must be male and thus the evidence of a woman is not admissible in these instances. This opinion is unanimously agreed upon by pre-modern jurists, including Imām *Mālik* , Abū Ḥanīfa, Shāfi'ī, and Aḥmad bin Ḥambal.[145]

The numerical strength of witness varies according to the nature of the matter. Matters related to Ḥudūd, involve right of Allah Almighty while financial and private matters include right of man.[146] In Ḥudūd offences where Right of Allah Almighty is involved, are the once which affect the society. Punishments of these offences are harsher and deterrent as compared to personal rights.

---

[141] Ibid,

[142] Mālik bin 'Anas bin Mālik bin 'Āmir , "al-Maūta' ", vol 5, (Abu Ẓahbī: Mūassasah Zahid bin 'Amir al-'Asbīhi, 2004), 1198.

[143] *Imām Marghīnānī* says that this punishment includes both right of Allah and right of man. So, the witness should conceal about right of Allah Almighty and it is obligatory to bear testimony about right of man. The witness should use the word "he took" (أخذ) Akhaza, instead of using the word "he stole" because if he used the word, he stole then he will be liable to hadd. But if he said he took than there are a number of reasons for taking something. This way the person will be saved from imputation of hands.

[144] *Al-Hidāyah*, vol. 3, 116.

[145] 'Abu Ḥussain Yaḥyah bin 'Abī al-Khaīr al-'Imranī al-*Shafi'ī*, "*Al- Bīyān fi-Mazhab Imam Shāfaī*", vol. 13 (Jaddah: Dār al-Minhāj, 2000), 324. This stance is adopted by all four school of thoughts because of the saying of the Prophet (PBUH).

[146] *Al-Hidāyah*, vol. 3, 116, Also in 'Abu Ḥussain al-'Imranī al-*Shafi'ī*, "*Al- Bīyān fi-Mazhab Imam Shāfaī*", vol. 13/324.

Essentially, there are four categories of testimony;

1. Testimony requiring four witnesses,
2. Testimony requiring two witnesses,
3. Testimony of one man and two women,
4. Testimony of woman alone

Islamic law requires testimony of four men in crime of fornication and slandering. All the other Ḥudūd offences and punishment of Qiṣaṣ requires two male witnesses. Two male witnesses are required in cases of commercial transactions. If two male witnesses are not available, then testimony of two women and one man is admissible. Testimony of a woman alone is allowed in the cases where presence of a man is very rare. The details of these categories are discussed below. [147]

2.3.3.5.1 Testimony of Four Men

Four witnesses are required in offence of *zinā* as ordained by *Qur'ān*. Allah Almighty says in the Qur'ān;

وَٱلَّٰتِى يَأْتِينَ ٱلْفَٰحِشَةَ مِن نِّسَآئِكُمْ فَٱسْتَشْهِدُوا۟
عَلَيْهِنَّ أَرْبَعَةً مِّنكُمْ [148]

"Those who commit unlawful sexual intercourse of your women - bring against them four [witnesses] from among you"

In case of fornication, number of witness is fixed to four. The reason behind this number is the seriousness of the nature of crime. The allegation on someone regarding this offence shall

[147] Al-*Qur'an* [4:15], Al-*Qur'an* [2:282]
[148] Al-*Qur'an* [4:15]

have grave consequences on his or her life and family. An un married person, if guilty shall be punished with 80 lashes. Married person shall be stoned to death. [149]

2.3.3.5.2 Testimony of Two Men

Testimony of two men are required in the following two cases;

1. Ḥudūd offences other than adultery and slandering (Qadhaf).
2. Financial and private matters

Allah Almighty says in *Qur'an*;

وَٱسْتَشْهِدُوا۟ شَهِيدَيْنِ مِن رِّجَالِكُمْ [150]

"And get two witnesses out of your own men"

This verse of *Qur'an* is a general one which includes *ḥadd* offences (except zinā and *Qazf)*, financial matters and private matters.

2.3.3.5.3 Testimony of One Man and Two Women

The general principle for testimony, is of two just men. But in exceptional cases where two men are not available testimony of one man and two women is admissible. All the matters

---

[149] 'Ubada b. as-Samit reported: Allah's Messenger (May peace be upon him) as saying: Receive (teaching) from me, receive (teaching) from me. Allah has ordained a way for those (women). When an unmarried male commits adultery with an unmarried female (they should receive) one hundred lashes and banishment for one year. And in case of married male committing adultery with a married female, they shall receive one hundred lashes and be stoned to death. Sahih Muslim, book 17 tradition number 4191.
http://www.iium.edu.my/deed/hadith/muslim/017_smt.html (Last Accesed July 19, 2019)

[150] Al-*Qur'an* [2:282]

require two men or one man and two women, other than Ḥudūd (except fornication and slandering) and Qiṣāṣ. Matters in this category involve nikāḥ, divorce, agency, property and financial matters, etc. [151]

Allah Almighty states in Qur'ān :

فَإِن لَّمْ يَكُونَا رَجُلَيْنِ فَرَجُلٌ وَٱمْرَأَتَانِ[152]

"And if there are not two men [available], then a man and two women."

This verse discusses exceptional cases where two men are not available then two women should testify against one man. This does not mean that women are so inferior that they equalize man by adding a number of two.

Qur'an describes the rationale of women's testimony as;

أَن تَضِلَّ إِحْدَىٰهُمَا فَتُذَكِّرَ إِحْدَىٰهُمَا ٱلْأُخْرَىٰ[153]

"So that if one of the women errs, then the other can remind her"

Allah Almighty says that the rationale of replacing two women in place of one man is that if one of them forgets the other one would remind her. Here the reason of forgetfulness does not mean that women have a weak memory. But the reason behind it is that financial cases and disputes arising in trade hubs and markets are not the workplace for women. The workplaces of women are usually homes and upbringing of their children, and not usually their offices or

[151] Abū Yūsaf al-Shīrāzī, "Al-*Muhazab fi al-fiqh al-Imām Shafi'i*", vol. 3, (Dār al-Kitab al-'Ilmiah, n.d), 450.

[152] Al-*Qur'an* [2:282]

d[153] Ibid.

trade hubs. She must not be very actively present in financial matters taking place outside in the market place. That is why two women are allowed to testify.

In this case, the testimony is to be borne by one woman only. The other woman is there to assist her and remind her about the incident. So, testimony is originally borne by one woman only. [154]

2.3.3.6 Conditions of Testimony in Islamic law

Another very special feature of testimony in Islamic law are the conditions of testimony. Islam does not admit mere testimony. It attaches certain conditions to it.

These conditions are very helpful in getting access to authentic evidence. Authentic evidence is very important in electronic evidence. So, these conditions would also be applicable in electronic evidence.

Imām Sarakhsi says that it is a religious obligation to admit testimony but for that, the testimony must be filtered by applying certain conditions.

Jurists have classified the conditions into two main categories;

1. Conditions for carrying or bearing of testimony (Shurūt at-taḥammul)
2. Conditions related to performance (Shurūt al-'Adā')[155]

Witness's personal knowledge about the subject matter of testimony is called *(taḥammul-a-shahādah)* or carrying of testimony. Tahamul, means capability of witness to retain testimony through observation, understanding of incident, inspection and memory.[156]

---

[154] Jarīr al-Ṭabri, *Jāmay' Al-Bayān fi Tā'wīl al-Qur'an*, vol. 6 (Beirut: Mūasasah- ur Risālah, 2000), 26.
[155] Alā' *al-Dī*n, al-Kāsānī, (d. 587H), *"Badā'i' al-Ṣanā'i fi tart īb al-sharā'i"*, vol. 6/ 266.
[156] Ibid.

While expressing that knowledge in front of the court is called performance of testimony ('Adā'-u- *shahādah).* It means capability of saying or uttering the words in court. Technically, when the witness stands before the court and acknowledges about the facts in his knowledge using the word 'I testify', that means performance of testimony. [157]

Imām Kasāni, in his book "Badāi'-wa-Sanāi'", states that there are number of conditions for witnessing. One of them is related to the qualification of witnesses, while another relates to the statements, few other conditions relate to the witnessed facts and events. He has discussed certain other conditions, which relate to the place of witnessing.[158]

2.3.3.6.1 Carrying/Bearing Condition (Shurūt at-taḥammul)

As far as the conditions for carrying or bearing of testimony (Shurūt at-taḥammul) are concerned, they are broadly categorized into two categories:

1. General or basic Qualifications
2. Special Qualifications

Both of them shall be discussed here.

2.3.3.6.1.1 General Qualifications

The Muslims jurists are of the view that admissible and competent testimony arises out of three main qualifications;

1. **Witness must be sane and adult**: An insane or a child cannot testify. The reason behind this is that reliable witnessing arises out of understanding of what has happened.[159]

[157] Ibid, 6/267
[158] Ibid.
[159] Kāsānī, *"Badā'i' al-Ṣanā'i'"*, vol. 6, 266.

2. **Witness must be a sighted person.** It is the view of the *Ḥanafī* scholars that the witness must be a sighted person. Shāfi'ī scholars, think that eyesight is not a necessary condition, as long as the hearing capacity is good. But *Ḥanafī* scholars argue that sounds can resemble other people as well. That is why they do not admit testimony of a blind person. For them relying on the hearing without capability of seeing is not sufficient.[160]

3. **Witness must have seen or observed the event directly:** It excludes the cases where witnesses have heard from someone else. Imām Kasānī says that jurist have stipulated this condition on the basis of saying of Holy Prophet (PBUH) for this condition, "If you know like the sun, then bear witness otherwise do not".[161]

Witnessing on the basis of widely circulated information, or a famous piece of information (tasāmu') is permissible only in cases of marriage, kinship and death because these matters lie within tne public domain. Allah Almighty states. "Do not pursue matters about which you do not have knowledge". [162] Scholars say that it is being stated about false testimony (Shahādah al-zūr). Some say that by pursuing means not to say.[163] Please explain the significance of this verse based on the book of tafsir

Imām Sarakhsī stated in his well-known book, al-Mabsūt, that hearsay by mean of widely circulated information is not allowed in the cases of property. He further added about the cases of marriage that as a general principle hearsay should not be allowed in cases of marriage. The reason behind it is the sensitivity of the cases. But it is permissible by way of istihsan in matters related to kinship, appointment of judges, marriage and death. [164]

[160] Ibid.
[161] Sarakhsi, *Al-Mabsūt*, vol. 16, 112.
[162] Al-*Qur'an* [17:36].
[163] Muḥammad bin Jarīr al-Ṭabri, Jāmay' al-Bayān, 17/ 448.
[164] Sarakhsi, *Al-Mabsūt*, vol. 6, 266-267. Also in, Kāsānī, *"Badā'i' al-Sanā'i"*, vol. 6, 266.

2.3.3.6.1.2 Special Qualifications

These conditions are specialized with respect to, the number of witnesses, their gender and their agreement in testimony. The matters related to the number of witnesses and their relevant conditions have already been discussed. [165] These include cases of testimony of Ḥudūd and Qiṣāṣ, requirement of four witnesses for slandering and two for theft, etc.

2.3.3.6.2 Performance Condition شروط الأداء:

Following are the conditions of performance;

2.3.3.6.2.1 Al-'Aqal (The intelligence or Sanity)

The first condition for bearing testimony is sanity or intelligence. The person who is not sane cannot observe and gain information. Therefore, he is not able to testify. He cannot be an effective witness.[166]

2.3.3.6.2.2 Al- Bulūgh (Puberty)

The next qualification is al-bulūgh. If a witness is a major, he can testify. It is agreed by the scholars that a child cannot testify. [167]

Imām *Mālik* is the only jurist who permitted child testimony in cases of injury and torn clothes in the playground because adult witnesses do not go to such places. He said that after they have left the playground their testimony shall not be admissible, because they may be changing stories or facts. [168]

2.3.3.6.2.3 Al-Ḥurriyah (Freedom)

The third requirement for a valid testimony is freedom. The testimony of a slave is not admissible against free person, because Imām Kasānī says, that act of bearing witness and

---

[165] These topics are discussed in detail under topic 2.3.3.6.2
[166] Kāsānī, *"Badā'i' al-Ṣanā'i"*, vol. 6/ 267.
[167] *Al-Mabsūt*, vol. 16,135-136.
[168] Ibid

testimony occurs in the course of transfer of authority and custodianship. But slavery is a relationship with owners. In case of testimony, witness is transferring the authority over to the judge to pass the judgment. But a slave does not have such authority. Imām Kāsānī further stated that slave has a duty to respond to the court whenever his testimony is required. As a result, his obligation towards the master will be neglected. He will not be able to perform duties of the master properly. [169]

2.3.3.6.2.4 Al-Nutq (the ability to speak)

The testimony given by a person who is speech-impaired is not admissible. This is the view adopted by the *Ḥanafī* and Hanbali jurists; giving testimony requires expressing it with the tongue.[170] The scholars are of the view that the words of the witness must be evaluated and considered in order to validate the testimony. A person who is mute has no diction at all. So, he cannot be a witness.[171] His testimony may be a cause of confusion because he brings proof by his actions, according to his own knowledge, which does not bring any knowledge. So there is a defect in his testimony as the gestures are not as strong as verbal expressions, although it is considered that he informs.[172]

On the other hand, Shāfi'ī and *Mālikī* jurists, maintain that the testimony given by a person who is speech-impaired is acceptable if the sign he has made is understandable. Shāfi'īs have said "the testimony given by a person who is speech-impaired is acceptable in matters that involve actions but not words." [173]

---

[169] Al-Kāsāni, Al-Badāey', vol. 6, 268.
[170] Ibid, vol. 6, 130.
[171] Ibid, vol. 6, 268.
[172] Al- Sarakhsi, 16:130.
[173] Ibn 'Abd al-Barr, *Al-Kaafee*, 464, also in al-Nawawī, *Raūdhat at-Tālibīn*, Vol. 8,231.

2.3.3.6.2.5 Al-Basīrah (The Ability to See)

It is also one of the most important qualification for a valid testimony. The testimony given by a blind person is inadmissible, according to Abū Ḥanīfa and Imām Muḥammad. They are of the view that testimony of a blind person is not acceptable even if he had eyesight at the time of his original witnessing of that particular event. But Imām Yūsaf is of a different opinion and he says that if a person was sighted at the time of original witnessing, then his testimony is admissible. But if the item about which the testimony is sought, needs to be visually identified at the time of bearing testimony in court, then his testimony is inadmissible unanimously. [174]

Purpose of testimony, according to Imām Abū Yoūsaf is to acquire knowledge about the matter in question or about the item or event which needs to be testified to; and that knowledge is acquired if the blind person had eye sight at the time of original witnessing.

Imām abū Ḥanīfah and Imām Muḥammad are of the view that the witness needs to recognize the plaintiff and to point him out at the time of testimony[175].

2.3.3.6.2.6 Good Memory and Understanding

A foolish person cannot testify. Similar is the case with a person who is very forgetful.[176]

[174] Sarakhsī, Al- Mabsūt, Vol.16,129 .
[175] Ibid.
[176] Sarakhsī, Al- Mabsūt, Vol.16, 113.

2.3.3.6.2.7 Legal responsibility (Takleef)

Legal responsibility means that the testimony of a minor and lunatic is inadmissible. Witness must possess sanity ('aql) and maturity (bulūgh) at the time of testimony. *Mālikī* jurists opine that child testimony is admissible in hurt cases, subject to certain conditions. For instance, the child must be male and a free person. And that thetestimony must relate to other children and not any adults. [177]

2.3.3.6.2.8 Just Person, Probity ('Adālah)

Muslim jurists have unanimously agreed that a witness whose testimony entails a judgement must have the quality of being '*adl* (that is, observing '*adālah*). This condition is essential for distinguishing truth from falsehood. Allah Almighty ordains the Muslims, "take for witness two persons from among you, *endured with justice*".[178] The insistence here is on the witness's devoutness and uprightness. It follows that the testimony given by a fāsiq is not acceptable in court of law.

Fāsīq is a term used in Islamic law for a reprobate person who neglects decorum in his behaviour (murū'ah) or lacks honour and proper behaviour. A fāsīq is unacceptable in a court of law. Imām Shāfi'ī defines fāsīq as the one who commits major sins *(*al-kabāīr*)* i.e who disbelieved Allah Almighty or Prophets or the Holly books, committed wrongful murder, drinks wine or steals, is involved in giving a wrong testimony or who has put wrong allegation on someone (Qazaf). Testimony of such a person is inadmissible.[179]

[177] Abū 'Umar Yūsaf bin 'Abdullah al-Qurtubī, "*Al-Kāfi fi fiqh al-Madīnah*", vol.2, (Riadh: Maktabah al-Riadh al-Ḥaditha: 1980), 908.

[178] Al- Qur'ān *[*65:2].

[179] Yaḥyah bin 'Imranī al- *Shafi'ī*, "*Al- Bīyān fi-Mazhab Imam Shafi'ī*", vol. 13, 278

Testimony of 'Ādil is a compulsory. Mālīk defined *'Adālah* as 'the one who avoids major sins *(*al-kābai'r*)*, returns deposits and has good dealing with people. His good deeds are more prominent than the bad ones. Testimony of such a person is admissible.[180]

Aḥmad bīn Ḥunbal defines 'Ādil as: who fulfils his duties (farāīḍ), avoids major sins (al-kabāi'r), and he does not insist upon minor sins. He has the quality of generosity and graciousness. *Shafi'ī* considers graciousness as a necessary condition. [181]

Imām Kāsānī states that a just person is the one who is not known as a wicked person. While the other scholars say that a just person is the one whose good deeds are not more than his bad deeds.

Islamic Law keeps a very strong check on evidence through witnesses with sound character (Ādil). The probity and just ('adl) characters of witness make the passage of justice much closer and faster towards truth and justice. These just witnesses act like a right hand of a judge. The responsible behaviour makes a quite a number of things easier for the judge.

2.3.3.6.2.9 ***Islam***

The majority of scholars, including Shāfī , Mālīk, and Abū Thaūr,[182] opine that a non-Muslim cannot testify. This ruling is the same irrespective of whether he is testifying for a Muslim or a non-Muslim. They rely largely on the commandment of Allah Almighty. Allah Almighty

---

[180] Al-Kasani, : 268.

[181] AL-Sharbīnī al-Shāfi'ī, *Mughnī al-Muḥtāj*, vol.6/391. Also, in Shams al-Dīn Abū 'Abdullah Muḥammad bīn 'Abdur Raḥmān al-Ṭārāblisi al-Mālikī, *"Mūahib al-Jalīl fī Sharḥ Mukhtaṣar al-khālīl"*, vol 6 (Dār al-fiqr, 1992)151. Also see Mansūr bin Yūnas bin Ṣalāḥ al-Dīn 'Idrīs Ḥambalī, *"Sharḥ Muntaha al-'Irādāt*, vol.3. ('Alim al-Kutub, 1993), 577.

[182] Ṭārāblisi al-M*ālikī*, *Mūāhib al-Jalīl*, 150/6, Sharbīnī, *Mughnī al-Muhtāj* 427/4.

says,: "And take for witness two persons *from among you, endued with justice*, and establish the evidence as before Allah."[183]

However, an exception that is recognised by some of the jurists relates to giving testimony regarding wills during a journey. The exception is such that, the testimony of a non-Muslim will be admissible in places where there were no Muslims who could have testified. Proponents of this view have relied on the verse of Qur'ān where Allah Almighty says: "O you who believe! Let there be witnesses between you when death approaches one of you, at the time of bequest, two witnesses, just men from among you, *or two others from outside, in case you are travelling in the land and the disaster of death should strike you.*[184]

Ḥanafī jurists are also of the view that testimony of a dhimmī in matters related to marriage of Muslim to a dhimmī woman is admissible without any issues.[185] It is also important to note that Imām Abū Ḥanīfa, Ḥammād 'ibn Sulaīmān, and different other scholars are of the view that testimony of a non-Muslim is acceptable if it be for another non-Muslim, irrespective of the fact that the two of them profess the same religion or they profess two different religions. The *Ḥanafī* jurists have conditioned it with another rule which is that if the two of them belong to the same country only then their testimony is admissible. Otherwise their testimony given by one of them for the other is inadmissible.[186]

2.3.3.6.3 Rejection of Witnesses/Rejection of Evidence

There are a number of sins which if committed by a person, will result in the loss of probity in a witness. Imām Kāsānī states following sins which are of this nature.[187]

He is of the view that a person used to of alcohol and singing loses the title of a just witness. Similarly. If people gather around singer for intoxication and he provokes people of

[183] Al- Qur'ān [65:2].
[184] Al- Qur'ān [5:106,].
[185] Ibn Nujaīm, *Al-Baḥr ar-Rā'iq*, Vol. 3, p. 97.
[186] Al-Maūsūah al-Qūītīah al-Fiqhīah, vol.26/223.
[187] Al- Kāsānī, 6: 268-270.

decadence then he is not just in character. Similarly, a person who keeps pigeons or plays chess is not just in character. He will not be treated just if he not only plays with pigeons but he draws evil omens from them. In case of chess, it is allowed in some school of thoughts but *Ḥanafī* jurist disallow chess because it is a game.

The above is so descriptive. It is best if the information is analysed in paragraphs rather than numbering

There are certain other reasons due to which the testimony of an otherwise eligible witness might be rejected. For example, the testimony of someone who has grudges against another person, whether he is a Muslim or not, his testimony has to be rejected. The Holy Prophet (PBUH) has said, "the testimony a deceitful man or woman, of an adulterer and adulteress, and of one who harbours rancour against his brother is not allowable." [188]

The same rule goes for testimony of a person who would testify for himself. His testimony will not be accepted if he is also the litigant, the reason being, he may prioritize his interest over cause of justice. It is stated by the early learned jurists that testimony of a partner is not admissible where he has a share. Testimony of a *Mudhārib* (dormant partner) is also not admissible where he has a share. Testimony of a lawyer in a case which he is going to plead is not admissible too. [189] In all these cases testimony of a person means he is testifying for himself.

Testimony of a master for slave is not admissible because money of slave belongs to the master and it is considered as testimony for one's own self. [190]

---

[188] *Abū Dā'ūd Sulaīmān al-'Ash'th, Sunan Abī Dā'ūd, vol.3 (Beīrūt: Al-Maktabah al-'Aṣrīah*, n.d), 306. Tradition no. 3600 Translated by: Salcem Marsoof, "Witness Testimony – Some Perspectives from Sharia'at Law Justice"

[189] Abū Muḥammad Maūfiq al-Dīn 'Abdullah 'Aḥmad bin Qudāmah al-Ḥamblī, *Al-Mughnī li-'Ibn-Qudāmah*, vol. 10 (Cairo: Maktabah al-Qāhirah, 1986), 167. Ibn 'Ābidīn, Muḥammad Amīn bin 'Umar, *"Hāshiyah ibn 'Ābidīn"* vol.5 (Beīrut:Dār al-fikr, 1992), 480.

[190] *Al-Mughnī li-'Ibn-Qudāmah* 10/174

It is agreed by few jurists that spouses are not allowed to testify for each other. This is the opinion of Sha'bī, Nakh'ī, *Mālik*, and Abū Ḥanīfah. On the contrary, *Shafi'ī*, Ḥassan, permitted testimony of a spouses for each other because they consider this contract, a contract of benefit *(manfa'ah)*.[191] Same is the case of parents and their off springs. Neither of them can testify for each other[192].

There is no such restriction in English law regarding the conditions of witnesses testify for their close relations. Spouses can testify for each other; sons can testify for their parents. The child's testimony is admissible. Qanūn-e-Shahādat does not specify any such condition.

2.3.3.7 Women's Testimony

It is unanimously accepted by the four School of thoughts that testimony of women is not acceptable in Ḥudūd and Qiṣāṣ cases [193], unlike ahl-Zāhir [194]. But this is not the case in financial matters where testimony of two women is admissible along with one man.[195] Imām Abū Ḥanīfa says that testimony of women is admissible in all matters, whether financial or not, other than Ḥudūd and Qiṣaṣ.[196] These matters include, marriage (Nikaḥ), divorce, freeing

---

[191] Ibid. Abū al-walīd Muḥammad bin Aḥmad ibn Rushd. "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*", vol. 4. (Cairo: Dār al-Ḥadith, 2004), 247.

[192] Sharbīnī. "*Mughnī al-Muḥtāj*". 6/390.

[193] Ibn Rushd. "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*". 4/ 247.

[194] Abū Muḥammad 'Ali bin 'Aḥmad bin Saee'd ibn Ḥazam. "*al-Muḥalā bil Āthār*",*vol. 8 (Beirut: Dā*r al-fikr, n.d), 478. It is stated by ibn Ha'zam that women's testimony is allowed in Hudud and Qisas cases. The reason for this ruling is that they do not believe in analogy. They say that if Allah Almighty has permitted women to testify in financial matters they are allowed to testify in all other cases. It is stated in his earlier quoted book: "In cases of adultery, it is not permissible to accept the testimony of fewer than four just, Muslim men, or in the place of each man, two just, Muslim women. Thus: three men and two women, two men and four women, a single man and six women, or eight women alone [without any men] may testify in cases of adultery. In all other cases, including hudud and qisās, marriage, divorce, the return of wives after divorce, and monetary matters, the tes timony of no fewer than two just, Muslim men, or a man and two just, Muslim women, or four just, Muslim women is acceptable. And in all of those cases except hudud a just man alone or two just women with an oath are acceptable. ibn Ḥazam, "*al-Muḥalā bil Āthār 8/476. Translated by* Karen Bauer, "Debates on Women's Status as Judges and Witnesses in Post-Formative Islamic Law". *Journal of the American Oriental Society*, Vol. 130, No. 1 (January-March 2010), pp. 1-21, 7.

[195] Al-*Qur'an* [2:282]

[196] Marghīnānī, *al-Hidāyah*, vol3/ 116. Also, in Ibn Rushd. "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*", 4/ 247.

of slave, 'Iddah and Ṣulḥ. When a woman is replacing man for testimony, two female testimonies shall be admissible.[197]

In the cases related to property, the condition is different. In cases of property, women's testimony is admissible.[198] While on the matters of kinship, marriage, divorce, etc., jurists are divided in their opinion. Ḥanafī jurists think that females are allowed to testify, while Shāfai jurists think the other way. [199]

Shafi'ī differ in this opinion and state that women's testimony is not admissible except in the matters pertaining to money. The reason according to them is that women's testimony is originally inadmissible due to their defect in understanding, incapacity of governance and lack of memory. [200]

Al- Marghīnānī is of the view that women can testify originally because a woman has the capability of managing everything which is required for testifying i.e. after watching the incident, memorizing it, and conveying the relevant information of the incident to the judge. According to al- Marghīnānī, it is immaterial whether they are deficient in 'aql. He says that *Ḥanafī*s allow women to testify due to the reason that they are capable of meeting the basic elements for testimony although their memory is not that good as compared to men in general. This problem of not being able to remember incidents properly, according to him, is guarded against by making a requirement of two female witnesses for every male witness.[201]

2.3.3.7.1 Single Woman's Testimony

---

[197] Ibid
[198] [Al Quran 2:282]
[199] Marghīnānī, *al-Hidāyah*, vol. 3/ 116. Also, in Ibn Rushd, "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*", 4/ 247.
[200] Al-Shīrāzī, "Al-***Muhazab fī al-fiqh al-Imām Shafi'ī***", vol. 3/437.
[201] Marghīnānī, *al-Hidāyah*, vol3/ 116 *Translated by* Karen Bauer. "Debates on Women's Status as Judges and Witnesses in Post-Formative Islamic Law", 7.

As far as the testimony of women alone is concerned it is considered acceptable by majority of the school of thoughts in the matters which are not exposed to men. These are the cases in which presence and testimony of men is usually not possible, as it does not involve inspection of men. For instance, matters related to child birth, menstruation, clarification of female sexual defects, etc. In these cases, the testimony of a single woman alone is admissible.[202]

Similarly, evidence of one woman is sufficient regarding virginity defects in private parts which cannot be exposed to men. This principle is derived from saying of Prophet (PBUH).

شهادة النساء جائزة فيما لا يستطيع الرجل النظر اليه[203]

"The evidence of women is valid with respect to such things as is not fitting for man to behold".[204]

In matters of child weaning (al-Radhā'h) *Abū Hanīfah* is of the view that testimony of women alone is not admissible because this is the matter which is disclosed to men.[205] The rule regarding virginity is such that when a man buys a female slave on condition of her being a virgin and afterwards he wants to return her because she is not. Another woman would examine her and give testimony. If she is not virgin, the buyer will have the option to rescind the contract. [206]

---

[202] Sarakhsī, *Al- Mabsūt*, vol.5/10`1. Also, in 'Ibn Rushd, *Bidāyatu'l-Mujtahid*, 4/248.
[203] Sarakhsī, *Al- Mabsūt*, vol.5/101.
[204] The Hidayah or Guide: A commentary on the Mussalman Laws, Trans. Charles Hamilton, vol. 2 (London: T. Benslay, n.d),668.
https://books.google.com.pk/books?id=Tq9CAAAAcAAJ&pg=PA668&lpg=PA668&dq=The+evidence+of+women+is+valid+with+respect+to+such+things+as+is+not+fitting+for+man+to+behold&source=bl&ots=0qwE6qEfc0&sig=BO3cBfegfjoysZxtz4sEMiWa9wU&hl=en&sa=X&ved=0ahUKEwjExraN2KrTAhUEVxQKHRY8BrAQ6AEIKTAC#v=onepage&q&f=false (acessed: 17th April, 2017)
[205] Ibn Rushd, "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*", 4/ 247.
[206] Sarkhsī, "*Al – Mabsūt*", Vol. 13/111.

However, there is a difference of opinion among the jurists about the number of women to testify for these matters in which men cannot participate. Imām Abū Ḥanīfa is of the view that one woman is enough to testify. Imām Malik requires testimony of at least two women. Imām Shāfi'ī requires testimony of four women in these matters because Allah Almighty has made two just women equivalent to one just man. So. for that purpose two just men can only be replaced by testimony of four just women. [207] ("If there are not two male witnesses, then a man and two women from among those witnesses who please you; so if one of the two women errs, the other will remind her").[208]

Imām Sarakhsī says that it is a fact that the basis for not allowing women to testify alone is their lack of rationale ('aql) and religion (dīn), which the Prophet of Allah (peace be upon him) described as "deficiency," thus creating doubts about its complete absence. Forgetfulness and errors are common in women, they make relatively more mistakes then men, and the inclination towards pleasure is usually higher in them. These are the serious problems with respect to testimony. So, by analogy women alone should not be allowed to testify alone. But this analogy is not used at all times because of the saying of the prophet (PBUH) which allows women to testify alone in matters which men cannot see. [209]

2.3.3.8 Authentication of Witnesses

Islamic law of evidence introduced a unique method of authentication of evidence. Muslim judges are at a duty to admit testimony. But there are always apprehensions that witnesses are lying or giving false testimony. For that Islamic law introduced two different methods of authentications;

1. To ensure the presence of number of witnesses as per criteria of verses of *Qur'an*

---

[207] Ibn Rushd, "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*", 4/ 247.
[208] Al- Qur'ān [2:282]
[209] Sarkhsi, *Al – Mabsūt*, Vol. 16. 114.

1. To check the character of witnesses (Purgation)

2.3.3.8.1 Number Criterion

The criterion of number of witnesses has to be strictly followed. Evidence is inadmissible if it does not fulfil the required number. *Qur'an* stipulates to ensure certain number of witness for each testimony. So, it is obligatory and a necessary condition.[210]

This quorum of witnesses is stipulated to authenticate the evidence. The speciality of Islamic law of evidence is that it does not allow every Tom, Dick and Harry to testify in court. The witnesses are supposed to be probable and just. Jurists have set strict standards of probity for the admissibility of witness. Number of witnesses is also prescribed to avoid inaccuracy and unreliability. Witness and testimony together protect the rights of people.[211] That is why the standards for witness to testify are very strict.

2.3.3.8.2 Purgation

The most important criteria for selection of witnesses is "'Adālah" (Justice). The witness in order to qualify for bearing a testimony should be Just ('Aadil). It is the moral uprightness of an individual. It is determined by the judge once and for all through a procedure of formal certification and screening. After screening a witness qualifies to give testimony. There is a consensus of all the school of thoughts that testimony of Just ('Ādil) must be submitted before the court. Qur'an stipulates that witness should be just and says;

[210] *Al Mabsut*, vol 16/114
[211] Ibid, 215.

وَأَشْهِدُوا ذَوَىْ عَدْلٍ مِّنكُمْ[212]

"And bring to witness two just men from among you and establish the testimony"

The above mentioned verse is about making a testimony of just witness when a person has decided to divorce a woman or to keep her (Rujū'). Testimony of a just witness is necessary in both cases. [213] Meaning of the word adal is balance (al-waṣṭ).[214] It also means true (haqq)[215] Elaborate on the above verse based on tafsir

Purgation means Tazkīyah in Arabic. It is a formal procedure which is carried out by the judge in order to check out the character of witnesses. If he possesses a good reputation, which means his good deeds are dominated in his personality upon the bad deeds, it means he is able to testify. There is a difference between moral uprightness (Adālah) and Purgation. Moral uprightness is the apparent character of a witness while Purgation is a formal procedure as stated earlier. There are cases when moral character (reputation) is acceptable. In other cases, purgation (thorough investigation of just character) is required.

Islamic legal system puts a great stress on purgation of witnesses. *Sharī'ah* places a strict condition for the admissibility of oral testimony i.e. to be from just witnesses. According to Imām *Sarakhsī,* the statement of just and probable witness (Shāhid 'Adil) is the only source of authentic evidence. [216]

English legal system, on the other hand, does not introduce any process of purgation of witnesses as such. Witnesses in English courts are cross – examined later on which makes the whole process confusing, lengthy and difficult. Purgation is a process which filters the

---

[212] Al-Qura'n 65:2
[213] Muḥammad bin Jarīr al-Ṭabri, Jāmay'al-Bayān, 23/ 444.
[214] Ibid3/145.
[215] Ibid 3/400.
[216] Sarkhsi, *Al – Mabsūt*, Vol. 16/112.

witnesses before coming to the court, making the whole trial and cross examination more authentic and reliable. This is a systematic procedure which ensures authenticity of evidence.

Various methods of authentication are used in English legal system which includes: oral testimony, documentary evidence, circumstantial evidence, expert testimony, etc, but there is no such procedure involved relating to the purgation of witnesses. Islam since its beginning has worked on making characters of people. It encourages the societies to produce trustworthy people. Earlier in the past when Islamic law was in dominant position around the world, purgation was an encouraging incentive for the people to have an honourable impression in public. It was therefore shameful for a person who could not testify in court, having title of not being just, fasiq or a person who has a bad reputation in society. [217]

The criteria for a just witness, however, differed according to different jurists. For instance, Imām Abū Ḥanīfa says that in case of Ḥudūd and retaliation, mere apparent probity ('adalah) of witness is not sufficient but purgation (Tazkīyah) must be made. For Ḥudūd and retaliation all possible measures should be taken to prevent the punishment. Therefore, it is a pre-requisite that in such a case the character of the witness must be strictly investigated.

Imām Yūsaf and Imām Muḥammad are of the view that purgation (Tazkīyah) must take place in all types of cases and not only in Ḥudūd and retaliation. Their opinion is based on the logic that decree of the judge (*Qādi*) rests upon proof and proof rest upon integrity of the witness. Besides, the investigation of integrity of the witnesses tends to preserve the decree of judge from annulment. The reason is that, if the judge passes a decree on the bases

[217] Wakin writes in her book, Function of Documents in Islamic Law that these people were counted among notable of town that a'yān al-nas or the ayān al bilād, Jeanette, The Function of documentary evidence in Islamic law, 9.

of witness with probable character and later on it is discovered that witnesses were lying, the judgement would be rendered null.[218]

Marghīnanī says that according to many scholars the difference of opinion between Imām Abū Ḥanīfa and his disciples is founded on the difference of times. People at the time of Imām Abū Ḥanīfa were more pious and probity was common in people. At the time of two disciples maybe due to expansion in territories, people changed and falsehood was visible in the society. That is why they ordered investigation of witnesses in all cases. Today the decision of two disciples is suitable because the level of fisq has increased among the people.[219]

2.3.3.8.2.1. Purgation Process

The process of purgation (*Tazkīyah*) is one of the exclusive specialities of Islamic law of evidence. It is a process of authentication of evidence. Authentication is one of the major hurdles to be crossed in English law. Authentication of evidence is done through oral testimony (witness with knowledge), circumstantial evidence, expert testimony and others.[220]

These above-mentioned methods of authentication are also employed in Islamic law of evidence. But the most spectacular method of authentication is applied by Islamic law that is purgation. Oral testimony plays the role of a backbone in entire law of evidence. It is correctly stated by Imām abū Yūsaf and Imām Muḥammad that the judgment of the *Qādi* is

[218] Marghīnānī, *al-Hidāyah*, vol. 3/ 118.
[219] Ibid.
[220] Circumstantial evidences are relied pretty much in Islamic law as well, e.g when Prophet (PBUH) gave judgement of Hadd punishment to a woman when she was pregnant before marriage. Caliph Uthman also ordered hadd punishment to a person from whose mouth smell of vine was coming. There are a large number of examples which will be discussed later on. Similarly, expert testimony was regularly practiced in classical Islamic court. *Qur'an* says: "فَسْـَٔلُوٓاْ أَهْلَ ٱلذِّكْرِ إِن كُنتُمْ لَا تَعْلَمُونَ "if ye realise this not, ask of those who possess the Message (Translated by Yousaf Ali)

based upon testimony. So, the credibility of witnesses must be checked and investigated before accepting them in trial.[221]

Islamic law has introduced two methods of purgation:

a) Secret purgation

b) Open purgation

At the time of Prophet (PBUH), open purgation was in practice. In this type of purgation witness and purgator were summoned together and witness heard the examination himself. But later on, open purgation was changed to secret purgation in order to avoid quarrels among witnesses and purgators. Imām *Yūsuf* said that open purgation is equivalent to creation of quarrels. [222]

Imām *Abū Hanīfah* says that it is permissible to ask one messenger for purgation and it is better to ask two. Imām Muḥammad says that purgation is not valid until it is performed by two.[223]

2.3.3.9 Primary Testimony

It is generally accepted rule that evidence and testimony given in the court of law should be direct and primary. Islamic law prohibits admissibility of hearsay evidence. It is unlawful for a person to testify about an incident which was not personally seen, sensed or observed by him. Even in direct evidence Islamic law puts very strict standards for the acceptance of testimony.

[221] Marghīnānī, *al-Hidāyah*, vol. 3/ 118
[222] Ibid.
[223] Ibid

Islamic law permits direct testimony only. But certain facts can be witnessed on the basis of public knowledge. The notion of public knowledge gives birth to hearsay in Islamic law.

2.3.3.9.1 Hearsay Rule and Exceptions

Hearsay is allowed in Islamic law in very few cases which are not hearsay in its real sense. Islamic law allows hearsay in the cases, which are famous enough. For instance, cases of birth or death are the ones which are known to many. Or the cases of kinship. [224]

Hearsay is allowed in Islamic law in a very few cases which are not hearsay in the real sense. For instance, al – Majellah states in article 1688;

"It is necessary that the witness should know personally that to which they depose, and that their evidence should be given in that way. It is not permissible for them to give evidence saying, "By hearsay, i.e. I heard from people."[225]

But if, with respect to properly being *waqf*, or to the fact of a person being dead, person gives evidence saying, "I have heard from trustworthy person", his evidence is held good. In matter of *vilāīat* and death and parentage, it is permissible for a person to give evidence by hearsay."[226]

To state simply, a person can give evidence on certain facts, on the basis of public knowledge. This is permissible without witnessing the event or the act, upon which the testimony is being made. It is called *Al-Shahādah bi-Tasāmay'* in Islamic law. So, one can produce evidence concerning, a person's descent, marital status or death, without actually observing or being resent at the time of his birth, his marriage contract or his decease.[227]

---

[224] Encyclopaedia if Islam, "Shahid", vol. 9 (Leiden: Brill, 1997), 208.
[225] *Majallah al-Aḥkām al-'Adalīah*. (Karachi: Kārkhāna Tijārat Kutub, n.d), art: 1688.
[226] Ibid.
[227] Encyclopedia of Islam, s.v. "Shāhid", (Leiden: Brill, 1997) vol.9, 208.

It is permissible to testify in these four cases on the basis of hearsay *(Al – Tasāmay')*. The purpose of allowing these cases is to avoid hardship (*Ḥaraj*). The above-mentioned cases are the ones which are directly observed by few but receive fame in society easily. For instance, news of someone's death is enough to testify about it, because only a few people are present at the time of death. But this news spreads fast that so and so person died. On the basis of spreading of news, it is allowed to testify about it.[228]

If someone sees that a person is sitting in a court room and a lot of people are coming to him for decisions. He is allowed to testify that he is a judge on the basis of hearsay. [229]

In Islamic legal system judge has the discretionary power to admit or reject any exceptions to the hearsay rule on the basis of credibility of hearsay. Marghīnanī says that analogically or as a matter of general rule, it is not lawful to give evidence on the basis of hearsay. The reason is that the foundation of testimony is entirely based on sight and direct observation. That is the only way of deriving knowledge. These exceptions are permitted on the basis of istiḥsān. [230] That means adhering strictly to the rule of hearsay creates hardship for the general public.

The above mentioned four cases, in which hearsay is permissible, are the ones which are seen or observed by a few people. These cases usually carry element of privacy. It will cause a great hardship for people at large if it is expected to have a direct testimony on these cases. That is why they are permitted by way of hearsay. For instance, birth is an event for which none is present but midwife. Marriages and deaths are seen by few and cohabitation is seen by none. From all these events a number of consequences arise. For instance,

---

http://library.ut.ac.ir/documents/381543/3581025/Brill_-_The_Encyclopaedia_of_Islam_Vol_9_San-Sze_.pdf (accessed: 19th April, 2017)

[228] Sarakhsi, *Al-Mabsūt*, Vol.16, 150. Maghīnāni, *Al – Hidāyah*, vol. 3, 120-121. Also in Kāsānī, Badā'i' al-Ṣanā'i , vol.6, 266.

[229] Ibid 371.

[230] Maghīnāni, *Al – Hidāyah*, vol. 3, 121.

consequence of birth is inheritance, marriage is dower and maintenance etc. So, a credible hearsay testimony is permitted to solve this problem.[231]

As compared to western law, Islamic law is very strict in hearsay testimony. There are a large number of hearsay exceptions which are permitted in western law. For instance, *Present Sense Impression, Excited Utterance, Existing Mental, Emotional, or Physical Conditions etc. There are almost 30 hearsay exceptions present in US law of Evidence*[232]. But in Islamic law only these four cases are allowed. In other words, western law is broad in allowing hearsay and Islamic law is very cautious and limited. It permits hearsay in only those cases which are already known by way of public knowledge. So, these cases are not hearsay in the strict sense.

2.3.3.9.2 Secondary Testimony

Another very interesting feature of Islamic law of evidence is secondary witness *(Shahādah 'ala Shahādah)*. Secondary evidence is completely different from hearsay evidence *(Al-Shahādah bi-Tasāmay')*. In this kind of testimony if the primary witness is either too far or is unable to attend the court for testimony due to any reason. He transfers his testimony to another just witness. He makes him his representative. This kind of testimony is permissible in Islamic law. In other words, if a witness has a legal excuse for not being able to attend the court session, he can transfer his testimony to other two just witnesses. It is called *Shahādah*

[231] Ibid.
[232] See Federal Rules of Evidence of USA. Rule number 803 "Hearsay Exceptions". (Accessed last May 24. 2017) https://www.law.cornell.edu/rules/fre/rule_803

bi-Tasāmay in Islamic law. However, secondary testimony is inadmissible in Ḥudūd offences or Qiṣāṣ.[233]

Imām *Abū Hanīfah* says that one secondary witness is enough for one primary witness. Two witnesses will testify in place of two.[234] But Imām *Shafi'ī* opines that two secondary witnesses will take the testimony of one primary witness and four secondary witnesses will testify in front of the judge for two witnesses. [235]

Imām Sarakhsī says this kind of testimony is allowed in all cases except Ḥudūd and Qiṣāṣ.[236]

2.3.3.10 Comparison in English and Islamic Law

The above-mentioned facts made it clear that the general principles of Islamic law of evidence are different from the English law. There are some major differences in English and Islamic law on oral testimony when purgation, hearsay and just characteristic of the witness comes under discussion. Secondly, the detailed conditions specified for the witness in Islamic law are not discussed in similar detail in the English law.

The standards of admissibility are somewhat similar in both the English and Islamic Law.

2.3.4 Documentary Evidence (Al-Kitābah)

Documentary evidence or al-Kitābah is a general term to represent a type of evidence which includes not only documents in writing but also maps, graphs, plans, photographs, etc.[237]

[233] Encyclopedia of Islam, "Shāhid", (Leiden: Brill, 1997) vol.9, 208.
[234] Al-'Aīnī, "*al-Bināyah Sharh al-Hidāyah*", vol. 9/127.
[235] Sarakhsi, "*Al-Mabsūt*", Vol.16, 138.
[236] Ibid 138.

A type of written proof that is offered at a trial to establish the existence or non-existence of a fact that is in dispute- letter contract, deed, license, certificates, tickets, are documentary evidence. [238] . It has to be kept in mind that documentary evidence is subjected to best evidence rule. It is required to present original document unless there is reason to do so. It is also passed through the test of authentication. That test is more rigorous in case of electronic evidence. [239]

Islamic law also pays great attention towards documentary evidence. *Qur'an* itself orders to write down the transaction or any debt which is to be returned.

2.3.4.1 Legal Validity of Documentary Evidence in Qur'an and Sunnah

Vast literature is present in classical Islamic law on documentary evidence. Kitāb al-shurut in classical *fiqh* books, is particularly relevant to the literature of written contracts and formularies, which after fulfilling certain conditions were binding upon the parties and was admissible in the court of law.

Jeanette Wakin writes in her book "The function of documents in Islamic Law" that there was a frequent practice of using written documents for private transactions. Almost all kinds of private documents depended on written documents for private transactions. The usage of documentary evidence though, not very extensive in the beginning, but was quite extensive later on as *Hanafi* law developed.[240]

---

[237] All the states have legislated in a way that they have expanded the concept of documentary evidence to electronic evidence as well. Pakistan is also an example in this regard, article 2(b)of Qanoon-e-Shahadat Order state that document can be a letter, figure, photograph or words printed. Due to this many judgments in Pakistan have linde article 2(B) with article 164 of Qanoon-e-Shahadat Order and said that the word document is implied to the evidences that are available because of modern devices. One of the leading case in this regard is *Sikandar Ali Lashari v. The State* (2016) YLR 62 KARACHI HIGH COURT SINDH. It was observed that the term document is expanded and includes CDs Usbs and other electronic evidences. See chap 6, para 6.3.3.

[238] Western Encyclopaedia of American Law, S.v "Documentary Evidence".

[239] US Legal, Documentary Evidence Law and Legal Definitions. http:www.definition.uslegal.com/documentary evidence. (Last accessed July 13, 2019)

[240] Jeanette Wakin. *The Function of documents in Islamic Law* (New York: State University of NewYork press, 1972), 7.

Legal validity of documentary evidence in Islamic Law is derived from *Qur'an* and *Sunnah*.

Qur'an

Qur'an explicitly in Surah al-Baqarah;

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوٓاْ إِذَا تَدَايَنتُم بِدَيۡنٍ إِلَىٰٓ أَجَلٖ مُّسَمّٗى فَٱكۡتُبُوهُۚ

وَلۡيَكۡتُب بَّيۡنَكُمۡ كَاتِبُۢ بِٱلۡعَدۡلِۚ [241]

"O ye who believe! When ye deal with each other, in transactions involving future obligations in a fixed period of time, reduce them to writing let a scribe write down faithfully as between the parties."[242]

This verse implies that the parties ought to write down the contracts which they transact during trade dealings and also to witness upon it.[243] This rule is a great principle of trade market, as it really helps saving the sides of both parties in terms of their payments and dues. If this rule is vigilantly followed, the chances of disputes shall be very low.

Sunnah

There are other textual sources, which supports the use of documents, such as the Ḥadith. A large number of Prophet (PBUH)'s traditions established the precedent, regarding the orders about drafting legal documents and their enforceability in the court of law. For instance,

[241] Al-*Qur'an* [2:282]
[242] Translated by Yūsaf Ali.
[243] al-Ṭabri, *Jāmay' al-Bayān*, vol. 6/ 45.

Prophet (PBUH) ordered his companion 'Ali to draw up a document in his name at location Ḥudaībīyah.[244]

Similarly, Prophet (PBUH) bought a slave from the companion and drafted written document. He commanded his representatives abroad to draft documents.[245]

These are the guiding principles given from *Qur'an*, which ultimately resulted in very cautious attitude of worthy Jurists who left no stone unturned to make sure that all the documents are free from all the lacunas and loopholes. Jeanette reports in her book about Imām Taḥāwi that he was quite conscious about legal formulation of the document. He wrote in his book Shurūt that the attorney must be legal experts or else if the document is not properly formulated, it will hamper the rights of public. For instance, unlawful division of inheritance or other debt matters.

Taḥāwī, says in his book "Al-Shurūt" that documents were a useful support of oral testimony in that they help keep the creditor and debtor from forgetting their terms of the agreement.[246] Imām Sarakhsī also spread light on a number of advantages of written documents on the start of his kitāb Al-Shurūt.[247]

2.3.4.2 Role in Classical Islamic Courts

Islamic law primarily relies more on oral testimony. The moral uprightness ('Adālah) of an individual was maintained by the judge (*Qādi*), through a regulated procedure of screening and formal certification. If a person qualified to be a witness whose testimony could not be

[244] Muḥammad bin Isma'il (d. 256), *Saḥiḥ al-Bukhari*, vol. 3 (al-Najat: Dār al-Ṭaūq, 2001),Bab: Kaīfa Yaktub, tradition no. 2698.
[245] Sarakhsi, *Al-Mabsūt*, vol. 30, 168.
[246] Abī Ja'far Aḥmad al-Taḥawi, *Kitāb al-Shurūt al-kabīr*, vol 1, 4. He mentioned many other benefits of written documents which are discussed from page 26-29.
[247] Al-Sarakhsi, *Al-Mabsūt*, vol. 30, 167.

doubted, then his statement was accepted in the court of law. This way there arose a permanent body of accredited witnesses, who not only testified for and against the claims, but they also became personnel of the *Qādi*.[248] The duties of these witnesses were to give testimony and furnish proof of proceedings and judgements of *Qādi*s.

The clerical staff of the court had the duty to record these proceedings and judgments according to specified pattern.[249] This practice of keeping documents in custody of judges gave birth to large piles of archives, which were used as judicial records. These records were authentic documentary evidence, which were generally used as a reliable piece of evidence.

Another group of works was sijīllāt and maḥāḍir, which were the formularies containing model document for *Qādi*s and clerks acting as notaries. More accurately maḥāḍir were the documents or written records of proceedings before the *Qādi*, i.e. minutes of the court. Sijīllāt on the other hand were the written judgements comprising *Qādi*'s decision. [250]

So, there were two types of documents, which were archived in the courts for record keeping. Sijīllāt and Maḥāḍir (pl. Mahādir). These two terms are defined below;

The literal meaning of the word "*mahdar*" is "presence or being present". It has two technical meanings; the first refers to the record of a legal case, which includes written declaration by the parties relevant to allegations and proofs that were recorded by Qāḍi. The terms used in

[248] Jeanette wakin, *The Function of documents in Islamic Law*, 7.

[249] This record of the court was known as *maḥāḍir* and *Sijillāt*. These formularies contained the model documents for use of qadi and his clerical staff who were acting in the capacity of notary as well. More accurately maḥāḍir were the minutes of the court. These were the record of the court proceedings which were written in front of the qadi. While, sijillāt were the actual written judgment of the qadi. The word sajjala means "drafting of a document". Jeanette wakin writes in her book that "it also meant the diploma of investiture of a qadi and a document drawn up by a qadi nominating a witness" [249] see in, Jeanette wakin, *The Function of documents in Islamic Law*, 11.

[250] Reem A. Meshal, *Sharia and the Making of the Modern Egyptian: Islamic Law and Custom in the Courts of Ottoman (Cairo*: Oxford University Press, 2014), 114.

the books of Islamic law refers to the same meaning in chapters of "*sijīllāt and Maḥāḍir*"[251] The second technical meaning of the word 'mahdar' refers to the technical meaning statements of witnesses and to the signatures of subashi (chief of police), chawsh (sergeant or guard) and muhdir (court process-server), who participated at the decision session with experts. The statements were formulated in text, written and arranged in such a manner to confirm the accuracy of document. Sometimes, written testimonials were called mahdars, which were later on used as evidence (hujjah).[252]

Sijil

The word *sijil*, literally refers to "to read to record, or to decide". Technically this term is used to refer to legal registers in which legal cases are recorded. These documents contain legal cases involving people's copies of *Qadis*' judgments, along with the diverse records relevant to judgment. These registers are called "*sijillāt al-shari'ah*", court books, minutes of the case or register of *sijillat or qadi's* register.[253]

Private and public documents were admissible subject to the oral testimony. [254] Jeanette elaborates that the reason of introducing witness system on documentary of evidence was the refusal to recognize the written documents. This system helped and improved a number of difficulties regarding the admissibility of documentary evidence. Otherwise, there were many apprehensions about the forgery of the documents. Jeanette said that a number of witnesses in a city carried out this practice greatly. At the same time witness played a significant social role in the Muslim society. She stated further as:

---

[25]' Fatāwa al-Hindīyah, vol. 6, 160.
[252] Ahmad Akgündüz, Shari'ah courts and Shari'ah Records: The application of Islamic Law in Ottoman State, *Islamic law and Society*, vol.16, no.2 (2009), 7. (Accessed August, 4, 2017) http://www.jstor.org/stable/40377991
[253] Fatāwa al-Hindīyah, vol. 6, 160. Also in Ahmad akgunduz, Shairah courts and shariah records, 7.
[254] Wakin, *The Function of documents in Islamic Law*, 8.

"The *Qādi,* who determined his good moral character, was able to ensure that Islamic standards would be maintained and carried forward. The function of witness was a religious one *(waẓīfa dījiyya,* as opposed to administrative) because he was attached to the Sharī'a court. And though in later times many people complained of their corruption, as members of the literate and professional elite of the urban bougeosie, they were persons to be emulated with respect to ethical and social standards, witnesses were counted among the notable of the town, the a'yān al-nās or the *a'yān al-bilād,* and were in touch with many of the economic and social concerns of the community. *Ibn Khuldun* hints at it when he states that witnesses were useful to the *Qādi* in finding out about the probity of other men in large and complex city. In short, he witnesses, a person certified to be of good moral character, penetrated the whole of society and was influential in preserving and spreading Islamic norms. The latent contributions, it made to Islamic society, together with a certain degree of social inertial and the operation of vested interests may help explain why he continued to flourish for so long."[255]

The body of persons played a vital role in helping *Qādi* and in determination of moral character of the witnesses. All the proceedings of the court were recorded by the administrative staff. The records reserved with the name of these accredited persons were reliable proof as (documentary evidence). [256]

2.3.4.3 Viewpoint of Schools of Thoughts

The four school of thoughts have their own opinion regarding documentary evidence. There is a consensus of admissibility of documentary evidence, because of the explicit verse of Quran regarding commandment of writing of a contract or transactions. But this consensus is not absolute. There are restrictions on the conditions and circumstances in which documentary evidence is admissible.

For instance, in *Mālikī* school of thought, documentary evidences were accepted under restricted circumstances; and after the approval of two qualified witnesses.

---

[255] Ibid.

[256] This record of the court was known as mahdadir and sijilat. These formularies contained the model documents for use of qadi and his clerical staff who were acting in the capacity of notary as well. More accurately mahadir were the minute of the court. These were the record of court proceeding which were written in form of qadi. While siillat were the actual written judgment of the qadi. The sajjalat means "drafting of a document". Jeanette Wakin wrote in her book that "it also meant to diploma of investiture of a qadi and a document drawn up by a qadi nominating a witness". See in Jeanette Wakin, *The Function of Document in Islamic Law,* 11

Ḥanafīs also accept written evidence. If there are absolutely no possibilities of falsification of document, and it has been preserved in archives of court, it is valid evidence. For instance, the *Maḥaḍir* or the minutes of court are admissible evidence[257]. Thus, it became a common practice to draw up such documents before *Qādi* and deposit them back in the court's archives for safekeeping.[258]

Written contracts were an essential part of the economic function at that time. They were even practiced in more private areas of life as well. For instance, emancipation of slaves, legacies, marriage contracts were routinely recorded in the form of written contracts.[259]

These contracts were supposed to be witnessed in order to produce during trial. Along with that, these contracts had to be drawn up in correct form. So, the professional witnesses usually exercised the role of notary as well. *Ibn Khudūn* describes the dual role of witnesses as under:

"In every city, [the witnesses] have their own shops and benches where they always sit, so that people have transaction to make can engage them to function as witnesses and register the testimony in writing." [260]

Encyclopaedia of Islam writes about the role of witnesses in classical period and states that the testimonies were recorded in deeds since very early. The main purpose of doing this so was authentication of evidence. It also helped parties to not forget the terms of the contract later on. It was a very helpful tool in the time of disputes:

> "Already at a very early period, testimonies of legal acts were recorded in deeds in order to preserve the exact wording of the act. However, since under Islamic law documentary evidence is not admitted, the deed itself does not furnish proof, but, in cases of litigation, the

[257] Al-Tāssi, *Sharh Majalla*, 211.
[258] Wakin, *The Function of documents in Islamic Law*, 9.
[259] Ibid.
[260] Ibn Khuldun, The Muqadaddimah, An Introduction to History, 3 vols. Tran. F. Rosenthal, vol. 1 (New York, 1958), 463.

testimonies given in court by the witnesses who have signed the deed. In order to avoid the danger that such testimonies might be rejected because the witnesses were not professional witnesses, whose *'adālah* had been established by the court, and who were called *shāhid 'ādil*, were employed for recording important transactions. They first appear in Egypt at the beginning of the 8th century A.D. These witnesses, who had a legal training, were appointed and dismissed by the *qāḍis* of the courts where they performed their duties. Their task, however, was more comprehensive than acting as notaries public, for they functioned in general as judicial auxiliaries and occasionally, with the *qāḍi's* authorisation, even as judges, and heard minor cases independently. The office of *shahādah* was often regarded as a training period for future judges. Strictly speaking, the profession of drafting deeds (*mūwaththik, shurūṭ*) and that of testifying to it could be separated. In practice, however, they were not, and the notary would put his signature under the deed as a witness, together with those of the other witnesses. Although the signatures of two witnesses would technically be sufficient, for greater security many more were placed in the document, sometimes up to 48. Often these testimonies were added years after the original drafting. Nowadays, with regard to those domains of the law where the Sharī'ah is applied, most countries have modernised the law of evidence e.g. by admitting documentary evidence. With regard to the testimony of witnesses, however, some of the classical rules are often maintained, such as the rule that the testimony of one witness does not count. In Morocco, the classical system of appointed 'udūl still exists. Some of the countries that have recently expanded the application of the Sharī'ah to fields such as criminal law, have also enacted legislation to reintroduce to some extent the classical rules of evidence."[261]

It is a fact that the system of oral testimony was established at a larger scale but documentary evidence was equally important for the courts. It helped the judges to prove a case having an equal strength. We have gone through some historical facts that proved the existence of a proper system of record keeping and archiving which gave birth to large number of documentary evidence.

2.3.4.3.1 *Shurūṭ* Traditions

There was a proper system of consulting witnesses for the sake of drafting documents which were to be presented before the court as documentary evidence, if required. The practices in the market of documentary evidences were even wider. Parties routinely drafted contracts before signing them.

[261] Encyclopedia of Islam, s.v. "Shāhid".

Practically, there were a number of advantages for consulting a witness/notary for sake of drawing up of document. The most important of them was, to have the technical knowledge to make a document sound, stylistically correct and recording a legally valid operation. Thus, the professional witness also acted as a legal advisor to his clients.[262] All the above practices resulted directly to the outgrowth of *Shurūṭ* literature.

Due to the increasing needs of business and market at that time, jurists developed a literature of *Shurūṭ*. This literature comprises of practical work which not only intended to discover or explain the law, but to help the *Qāḍi* and other concerned persons in the application of law. Jurists compiled a number of handbooks or formularies, which were designed especially for the professional notary and consisted of model contracts which were legally correct for all possible needs.[263] The task of the notary was to fill in the "blank spaces", and add the witness signature.[264]

These formularies, by their nature were closely connected to *Shurūṭ* literature. In fact, they are usually given as a separate chapter at the end of the *Shurūṭ* literature. Author of one subject usually composed a separate writing on the other. The major difference among them is that *sijīllāt* and *Maḥāḍir* are not private and *Shurūṭ* are the private contracts saved in the court archives.[265]

---

[262] Wakin, *The Function of Documents in Islamic Law*, 13. Jeanette at one place states that there was no importance of documentary evidence in Islamic law and at other place he writes a whole book about the reliance of Muslim community on documentary evidence.
[263] Different Jurists Compiled books on *shurūṭ for instance, Sarakhsī, Ṭaḥāwī, Marghīnāni*
[264] Wakin, *The Function of Documents in Islamic Law*, 10.
[265] Al-Fatāwa al-Hindīyah, 2nd Ed. Vol. 6 (Dār al-Fikr, 1310H), 160.

> recommendation.....practice admissibility of written documents was at its lowest threshold and they were not considered as authentic and admissible evidence." [276]

The interesting fact is that all her research in this book explores the trends and practices for admissibility and formation of written documents. All her research is proving this statement wrong. For instance, at one place she discussed that there was an industry of witnesses who were experts of drafting legal documents. It was their expertise and they served as legal advisors as well. People used to come to them in normal routine for drafting of contracts. If her statement about inadmissibility of documentary evidence is correct, then the historical facts which are mentioned in her book and other texts are incorrect, which is impossible.[277]

Another article written on the same subject titled "A paper economy of faith without faith in paper: A reflection on Islamic institutional history" by Ghislaine Lydon[278] clearly states that;

> "Somewhat of a paradox that in all of the schools of Islamic law, written documents were not considered to be legitimate sources of evidence. Indeed, legal professionals such as Muslim judges generally did not admit documents, including contracts, as evidence in legal proceedings. This is because, in accordance with Islamic legal practice, evidence could only be oral in nature. In other words, evidence was represented by oral testimony derived from witnesses and not from written sources. Contracts, for instance, could not be used in a court of law without the presence of the witnesses attesting to the original agreement. The fact that Muslims did not assign legal personality to written documents surely complicated certain social and economic transactions. The reliance on witnesses for recognition, deliberation or enforcement of contracts would have posed particular problems to those involved in long-distance trade, such as principal investors and travelling associates typically located in geographically dispersed markets. As several scholars have recognized, the restriction

[276] Ibid, 6.
[277] Ibid, 7
[278]Ghislaine Lydon, "A paper economy of faith without faith in paper: A reflection on Islamic institutional history," *Journal of economic behaviour & organization* 71, no. 3 (2009): 647-659.

placed on written documents contradicts the *Qur'an*'s explicit endorsement of the recording of contractual agreements" [279]

After stating the legal validity of documentary evidence from Qur'ān and *Sunnah* there is no doubt that documentary evidence is admissible in Islamic law when Qur'ān orders to write down the debt transactions and make some one witness over that transaction. English law adopts the same methodology from accepting documentary evidence. The terms and condition of a contract are written on a piece of paper and then two witnesses testify and sign it. Oral testimony on documentary evidence is a common practice in Islamic as well as common law practice. So, it is incorrect to state that Islamic legal system trusted on oral testimony and not on documentary evidence.

The argument that common law admits public document without oral testimony and Islamic law does not, is wrong. We have examples in the books of classical Islamic law where Imām *Yūsuf* and Muhammad gave *fatwa* about the judgments archived in the cabinets of judges as admissible without oral testimony. The reason for admitting such documents was that their chain of custody.[280]

These types of writings about Islamic law are not based on reality as they do not carry any weight and proof. The practical side of this view point is different. Below are the details of practices of legal weight, age given and uses of documentary evidence in Islamic law and markets of that time.

2.3.4.6 Advantages

[279] Ibid, 648.

[280] Muhammad Khalid Al-'Atāsī, Shar*h Majallah al-Ahkām al-'Adaliah*, 5 vols. (Quetta: Maktabah Islamiah, 1985),

Imām Taḥāwī starts his book Jāmi'al-kabīr with a comparison of merits of oral testimony and written documents. Confining him to the two types of transactions mentioned in 2:282 of al-*Qur'an*, contract of sale with delayed payments and immediate payments (Tijārah Ḥaḍirah, lit. present trade), he comments that Allah Almighty has not made it obligatory to write the, second type of contracts, because it would have been oppressive. No one would buy anything even food or water without feeling obliged to draw a written document. However, Allah Almighty did recommend calling the witness in case of both types of sales because they could testify later if the merchandise had to be returned to seller due to defects or prior claims.

1. The purpose of writing a debt is to eliminate the distrust and forgetfulness, then a document of *shahādah* ought to be drawn up for all contracts of sale for the same reason. [281]
2. When the contract is carried out, the document may contain clauses which binds the parties in future. Some of them are not necessarily linked to a valid sale, but they ensure complete performance of the contract.
3. Recording the necessary details of contract in writing not only minimizes the chances of conflict between parties but also establishes the validity of transaction. Hence, no third party would likely to appear to challenge the sale that it was irregular or invalid.
4. It reduces the possibility of conflicting testimony on the part of witnesses in case they were called upon to testify in a lawsuit.
5. If they should die or be distant from the town where the litigation takes place, the practice of secondary witnesses (*shahāda 'alā shahāda*) to affirm the testimony of

[281] Imam Sarakhsī is more specific on this point. The document prevents disputes because it can be referred to in case of parties try to repudiate the rights of others. In this case the documents can be produced, the witnesses testify, and the deception is exposed.

primary witnesses solved this problem for the time being. [282]. But eventually, the document itself bearing the signatures of the parties will have to be consulted.

2.3.4.7 Electronic Evidence

Keeping all of the above facts in mind, it is clearly proved that documentary evidence has received great attention from the Islamic scholars and it is also obligation on Muslim in contracts by the command of Allah Almighty[283]. Electronic evidence has very close resemblance with documentary evidence. The documents that are based on internet and computer has a complete history which tells about the creation, modification or deletion of any document. So, this technology makes it more reliable.

It is accepted worldwide that electronic evidence is documentary evidence.[284] That is why electronic evidence is acceptable in Islamic law because Islamic law heavily relies on documentary evidence.

Of course, this does not mean that Islamic law would believe in Electronic evidence blindly. The modes of authentication would be applied to electronic evidence. For instance, oral testimony on electronic evidence, the provenance and chain of custody would also be established. Expert testimony will also be acquired where necessary.

Documentary evidence has prime importance in the field of electronic evidence as well as Islamic law. Islamic law not only admits documentary evidence but *Qur'an* commands to draft a document at the time of making a contract.

---

[282] Sarakhsī, *Al-Mabsūt*, vol. 30, 168. Imām Sarakhsī rightly remarks that heirs of the parties will want to know the contents.
[283] Al-*Qur'an* [2:282].
[284] *Sikandar Ali Lashari v. The State*, 2016 YLR 62 Karachi-High-Court-Sindh, *Rollo (William) v HM Advocate* 1997 JC 23, 1997 SLT 958 (HCJ).

That is why element of documentary evidence is common between both electronic evidence and Islamic Law. So Islamic law permits electronic evidence. But the restriction involved in admissibility of documentary evidence must be observed while accepting electronic document.

2.3.5 Expert Testimony

Another one of the most important mean of proof is expert testimony. The reference to this means of proof is very significant to be studied here as it is one of the most important factors for the admissibility and proof of electronic evidence. [285] Electronic evidence has a close relation with expert testimony. Because there are so many issues relevant to computer forensics which are technical. These issues can be better understood by an expert in the relevant field. Islamic law admits and accepts expert testimony. But electronic evidence cannot be perceived and interpreted without experts.

2.3.5.1 Opinion/Judgment of Prophet (PBUH) and Companions of Prophet (PBUH)

Expert witnesses has had an important role in Sharī'ah courts as well. The rationale behind is well illustrated by the following Islamic legal maxim "With respect to each craft, seek the assistance of the best practitioners of the same craft *(ista'īnū 'alā kull ṣan'a bi-ṣāliḥ ahlihā)*."[286] This maxim is a quotation of a tradition of Prophet (PBUH) from when the Companion of Prophet, Sa'd b. Abī Waqās, got ill and Prophet (PBUH) came for treatment. The condition of the patient was not good enough and Prophet (PBUH) realized that some

[285] For a comparative analysis on expert testimony in common law refer to topic 2.3.2.2

[286] Ismail bin Muḥammad al-'Ijloni al-Jarahī(d. 1162 H). *Kashf al-Khafā' wa mazīl al-Ilbās 'Ama Ishtahar min al-'A ḥadith 'ala 'alsina al-nās*, vol.1 (Al-Qairo: Maktabah al-Qudsi, li Sāḥibuha Ḥsām al-Qudsī, 1351H), 122. Also, in Ron Shaham, *The Expert Witness in Islamic Courts: Medicine and Crafts in the service of Law* (London: The University of Chicago Press, 2010), 27.

expert needs to examine him. That is why, he called upon al-Ḥārith b. Khlādah from the tribe of Thaqīf, who was known as an expert physician (*rajul yuṭabbib*) at that time.[287]

The basic rule which relates to the accommodation of modern means of proof, including forensic evidence, is founded in a tradition of Prophet (PBUH), in which he declared, as part of his universal inauguration of Islamic legal proceeding, that technical knowledge and human expertise are something other than revelation. Technical knowledge needs to be proved after proper foundation of evidence and proof. This can be proved by his famous saying in which he declared that: "Since I am only a human, like all of you, I might, when litigants come before me to decide between them, rule in favour of more eloquent of them. If I thereby transfer to him what is rightfully his brother's, I warn him to take not that which is not his, or I shall reserve for him a piece of Hell."[288]

This saying illustrates, that the issues of proof and evidence belong to human rationale and reason. Resultantly, its simplicity and complexity, depends upon advancement in field of technical knowledge to ensure justice. There are traditions of Prophet (PBUH) which permits and admit to take assistance of experts on the matters which are beyond the reasoning and knowledge of a layman.[289] from book of tafsir al-hadith

The reason why experts were indispensable to the judges was that, some indications (adilla, adillah sg. Dalīl) was only known to the experts through professional experience. Only they could testify as to the existence of things which were hidden from the layman's eyes. It is phrased as man lahu al-baṣar [or al-naẓar] fī dhālik al-bāb, in Islamic law books.[290] For instance, Imām Sarakhsī states if a woman is accused of adultery and she says that she is

---

[287] Khair al-din bin Maḥmood al-Zirkili al-Damishki (d. 1396). *Al-'A'lām*, vol. 2 (Dar al- 'Ilm lil-Malāyen: 2002), 157. Harith bin Kalādah was the companion who visited Persia and studied medicine from there. Prophet (PBUH) used to call him to see the patients when it was required.

[288] *Saḥiḥ Muslim*, Vol. 3, 131. Bab: 'Ism man khāsamah fil batil wa hua ya'lamhu, Tradition no. 2458.

[289] For instance, tradition of Holy Prophet regarding his companion Harith bin Kalādah is mentioned above. Prophet (PBUH) used to call him to see the patients when it was required.

[290] Sarakhsī, *al-Mabsūt*, vol. 9, 73.

pregnant. Her testimony will not be admissible until she is inspected by female experts. Expert testimony would be the basis for delaying her *ḥadd* punishment till delivery and lactation. [291]

Similarly, in al-Mabsūṭ, Imām Sarakhsī[292] justifies the recommendation to judge to consult expert witness, on the general principle given by Quran;

فَسْـَٔلُوٓاْ أَهْلَ ٱلذِّكْرِ إِن كُنتُمْ لَا تَعْلَمُونَ [293]

"Ask those who know [ahl al-dhikr] if you do not know".

The late *Ḥanafī* Jurist Ṣāliḥ b. Muḥammad Al-'Umarī (known as Fullan; d. 1803), the author of Iqāẓ HImām Ūlī-Abṣār li'l-Iqtiḍā, uses the ḥadith literature to strengthen his interpretation of the Qur'ān in term ahl al-ẓhikar as meaning "experts". According to tradition, one of the Muslim Warriors, after getting injury on head by a stone, asked his comrades-in-arms for the permission to use sand instead of water (taīyammum) for taking bath before prayer. But the permission was not granted. He washed his head with water and died. When Prophet (PBUH) was informed about this incident he got angry and said if the warriors were ignorant about something, they should have consulted experts. Al 'Umari concludes that, since the Prophet and his successors used to consult experts, the Shari'ah directs rulers and judges to consult experts as the physiognomic (qāif) and the assessor (Kharis).[294]

All the above examples clearly show that neither the Prophet (PBUH) nor the companions denied the importance of expert testimony. They inquired and investigated with

---

[291] Ibid.
[292] Sarakhsi, "al-Mabsūt", vol. 9, 103.
[293] Al-*Qur'an* [16:43; 21:7]
[294] Ṣāliḥ b. Muḥammad Al-'Amrī [known as al-Fullānī], *Iqāẓ Himam Ūlī-Abṣār li'l-Iqtiḍā' bi-sayyid al-Muhājirīn wa'l-Anṣār* (Beirut: Dār al-Ma'rifa lil-Ṭibā'a wa'l-Nashr, n.d), 121-22.

the means of modern proofs whatever was possible at that time. Today the case of computer forensics or electronic evidence lies in the same category. It is as per requirements of *Qur'an* and *Sunnah* that we should investigate them to whatever extent possible and should rely on expert opinion and modern means of proofs.

There are large number of examples which are present in the life of Companions and other scholars where they used their investigative skills to reach the truth. Such as when 'Ali (God be pleased with him) convinced Caliph 'Umar about a case which required an expert testimony. There was a woman in Madina, who fell in love with a man who rejected her wooing. She wanted to take revenge on him. She made a plan of making him liable for punishment. She spilled the egg white on her clothes and thighs and then complained to Caliph 'Umar b. al-Khattab that the man had raped her. 'Umar was about to pass judgment against that person, 'Ali b. Abi Talib intervened. After putting boiling water on the liquid, which according to plaintiff was the semen of the defendant. He identified the real source of liquid and urged the plaintiff to confess, which she eventually did.[295]

The Prophet (PBUH) decided about the paternity of a baby on the basis of bedding (firāsh). [296] Imām *Mālik* considers pregnancy as circumstantial evidence for adultery, if the girl is unmarried. In this case *ḥadd* punishment may be applicable. On the other hand, *Ḥanafī*, *Shāfi'ī* and *Mālikī*'s rejected application of *ḥadd* punishment, due to existence of doubt (*shubha*). According to *Ḥanafī* jurist Sarakhsī, if a woman admits that she is pregnant and she is unmarried, her claim would be verified by two female experts. If expert's answer is positive then her *ḥadd* punishment would be postponed for two years, during which she

---

[295] Anwar Mahmud Dabur, *al-Qara'in wa Dawruhafi al- Fiqh al-Jina'i al-Islami* (Cairo: Dar al-Thaqafah, al-Arabiyyah, 1985), 215. See also, Isam Gihanem, *Islamic medical jurisprudence* (London: Arthar Probsthain, 1982), 29.

[296]

would be imprisoned. If she is unable to deliver the baby during that time, *ḥadd* punishment shall be applied.[297]

It has also been reported about Prophet (PBUH) that he ordered a woman to be flogged on finding her pregnant while she was still unmarried.[298] Accordingly, the Prophet (PBUH), by these decisions, has established undeniable precedents to serve as instructive stare decisis for his Ummah (followers) regarding the leading matters of interest to the forensic sciences or electronic evidence long before they even came into existence. These decisions can also serve as a precedent in field of digital and computer forensics. [299] There are certain things which cannot be seen by a layman's eye but long practices of experts prove that they exist.

It is also known fact that in today's society, the use of electronically stored information has become deep-rooted and unavoidable. Without it, the infrastructure of all government and non-government institutions can collapse. Their method of proving is also becoming known and the discrepancies involved are also curable. So, in order to avoid admitting them on the grounds of not having direct linkages, it is better to have a fool proof system of admissibility of electronic evidence in the light of *Qur'an* and *Sunnah.*

The succeeding generation of jurists have also ruled on issues of great significance in the field of forensic evidence, under the heading of expert opinion (*Al-ray al-khabīr*). For instance, to decide on the virginity or otherwise of a woman, they required the wet nurse's opinion; to determine the amount of compensation for injuries, they sought opinions from the doctors, to allow the return of consumer goods on account of latent defects, they sought the

---

[297] Sarakhsi, *Al-Mabsūt*, vol. 9, 73.

[299] Sayed Sikanadar Shah Haneef, "Modern means of proof: Legal basis for its accommodation in Islamic law" *Arab Law Quarterly* 20, no. 4 (2006): 340

help of specialists to prove it, to name a few. According to their *ijtihād*, expert opinion, aside from the *Sunnah* and the practice of the companions, derives its validity from the Qur'ānic anecdote about Prophet *Yūsuf*.[300]

2.3.5.2 Authentication of Expert Testimony in Islamic Law:

There was a debate among the scholars regarding the probability of expert witness. Expert witnesses is sometimes referred as a term testimony (*Shahādah*), sometimes as a report (*Khabar*). The question arises as to when the jurist considered expert testimony as a *khabar*, in which one witness is required and when is it considered as a *shahādah* in which two witnesses are required.[301]

If one witness is sufficient, then the juristic justifications for relaxation of evidentiary requirements should be known.

There is a difference of opinion among the scholars regarding whether the expert testimony should be treated as a testimony or a report. There are a large number of examples quoted in classical Islamic Law and are discussed in chapter 2, in which the jurists have differed in opinion as to the requirement of number of witnesses in each matter.

For instance, in the matter of defects of slaves, *Imām Sarakhsī*, explicitly states the testimony of two expert witnesses are required because their report is binding on the judge as testimony. *Mālikīs*, also are of the view that two male expert witness are required. Though a minority view supports the stance, that one witness is enough, but the general view of the school is that two witnesses are required. [302]

300

301 Ron Shaham, *The Expert Witness in Islamic Courts: Medicine and Crafts in the service of Law* (London: The University of Chicago Press, 2010), 44

302 Ibn Rushd. Abū al-walīd Muḥammad bin Aḥmad. *Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*. 4 vols. (Cairo: Maktabah Ibn Taimiyah, 1987), 1037-1038

Similar debate is there in the matters related to evaluation of property, value of damages to both movable and immovable property and rental prices, etc. *Ibn Abidīn* requires testimony of two expert witness. He is of the view that two experts from the same field shall report. Imam *Sarakhsī* is of the opinion that if the matter pertains to the value of the stolen property, two witnesses are required. He says that if both the experts differ in their opinion and one says that the amount is less than *nisāb* of theft i.e. ten dirhams, and the other says it exceeds *nisāb*, then the *ḥadd* punishment for theft will be prevented due of presence of doubt (*shubha*). [303]

Imam Malik permits testimony of one witness in matters related to property. The *Māliki* jurist Qarāfi disagrees with *Mālik*. They are of the view that assessment is more similar to testimony than transmission.[304]

The divider (Qāsim) was an expert whose role was to divide estates and goods among partner and heirs. Imam Malik says that one divider is sufficient but two are better (Al-Aḥsan)[305].

Similarly, this difference of opinion is present in many other matters. Like physiognomy (qiyāfa). In this matter Mawardi (*Shafi'ī*) thinks that the judge will decide whether the expert witness will act as a judge or a reporter. *Mālikis* think that he is a reporter so one is enough.

Examination of the Islamic law clearly shows that sometimes jurists treat expert testimony as report and sometimes as witness and require number of experts explicitly mentioned in *Qur'an* and *Sunnah*. Sometimes Prophet (PBUH) relied on the opinion of one expert. Like Zaid b. Thabit translated Jewish scriptures for Prophet (PBUH). Such cases

[303] Ron Shaham. *The Expert Witness in Islamic Courts* 44
[304] Ibid. 45
[305] Ibid.

encourage the jurists to make an opinion on the expert testimony just like a matter as transmission of Hadith. Which means one witness is enough. [306]

But the factor of necessity is also very important element for demanding one witness. As for the traditions of Prophet (PBUH), there was the fear of losing the binding dictums of Prophet (PBUH). So, the tradition of one person was validated. Similarly, matters related to rituals, there was a fear of prejudicing God's right. Finally, with regards to expert witness, one testimony was allowed because it was sometimes impossible to find two qualified, just expert witnesses in each case.[307] Mostly, jurists require two experts in majority of cases (including women's related matters) to increase the probability of witness. But they were ready to adjust with single testimony at the time of necessity (*Darūrah*).[308]

The jurists in order to find out a logical reasoning for the probative value of expert witnesses, had to search a lot. For this they made a difference between transmission of Hadith and court testimony. Since the expert testimony comes in the middle of both. So, they tried to dig out the similarities for each expert testimony with that of the transmission of Hadith and court testimony. If they found that the similarity of expert testimony with the transmission is more, they concluded that one expert was sufficient. If the similarity of the expert testimony was stronger with court testimony, they concluded that two witness are required. [309]

As a general rule, more prevalent juristic opinion was that the expert is a witness. A doctor's opinion of the "age" of physical defects found in a slave whom he bought is a good illustration. The *Ḥanafī*, *Mālikī* and Ḥanāblīs opine that at least two physicians must report for the defects, only then annulment of the sale contract will take place.[310]

---

[306] Ibid, 53.
[307] Ibid.
[308] Sarakhsi, *al-Mabsūt*, vol. 13/ 110.
[309] Ron Saham, *Expert Testimony*, 54-55
[310] Sarakhsi, *al-Mabsūt*, vol. 13/ 110.

Many of the jurists who concluded expert as witness and permitted testimony of one witness on the ground of necessity (darūra). They allow it as an exception. Necessity was introduced because there was a problem of finding quality experts in every geographical area, in a number which would satisfy the needs of judges. The jurists were aware about the practical problem, and knew that insisting on number of experts strictly will stifle the judicial system.

Same is the case with female expert testimony. The scholars who considered the report as *khabar* were ready to rely on single female expert, but they preferred to have two, for having higher reliability. The jurists who considered it as court testimony required two experts. But they were ready to accept one on the grounds of necessity which is unavailability of more than one expert.

2.3.5.3 Modern Expert Testimony

The journey for ensuring the probability of experts in Western legal system is quite different from Islamic law. The two main elements of Western Modern Natural Sciences in expert witnessing are as follows;

1. Scientific dictums must be based on facts derived from experiments
2. Scientific laws and factual dictums must be quantified and mathematically presented

The modern approach towards sciences has brought "explosion of facts" in modern western law that has resulted in tremendous growth in use of expert testimony. The field of knowledge whose expertise is required for testimony has become highly area specific. The

general attitude in modern day towards growing scientific knowledge is that, there is a growing expectation regarding the possibility of fact determination.[311]

The change in United State and European expert testimony is due to the reform in legal procedure and scientific knowledge. In an excellent research on history of expert testimony in British and U.S legal systems between eighteenth and twentieth centuries, Tal Golan writes that "Science and law are mutually supporting belief system and deeply connected social institutions heavily invested in each other". [312] Day to day advancements in scientific knowledge brings new forms of knowledge to court in days and weeks. This scenario has challenged the judicial practices and it has inspired the development of evidence rules.

In twentieth century, the expert's qualification and role in US legal system is identified by Fryer dictum. This rule asserts the accepted position of experts in relevant scientific community. Later on, on 1993, The Daubert precedent, replaced the Fryer rule. This rule added four more criteria to the one prescribed by Frye. These are, testability, peer review, error rate, and standardization. In this precedent, the court is supposed to analyse the scientific mode of thinking and the method by which conclusion is achieved. The expert who is appearing before the court must convince the judge that the general theory he is relying on may be verified by means acceptable to the court, and that this theory is capable of predicting.[313] According to another view, the role of court is not to achieve a cosmic understanding of the sciences but to be assisted by scientific knowledge to the extent required for solving the judicial disputer under review.

---

[311] Ron Saham, *Expert Testimony*, 12
[312] Tal Golan, *Laws of Men and Laws of Nature: The History of Scientific Expert Testimony in England and America* (Cambridge: Harvard University Press, 2004), 2.
[313] Ibid, 247-264.

2.3.5.4 Precedents in Islamic Courts

Experts have been playing a very active role in Islamic courts. They were consulted whenever any help was required from them. The matters on which their help was taken range from economic matters to physical injuries. In fact, there is a long list of experts who were acting as a right hand of *qādis*. For instance;

1. Experts in the relevant fields of economics were consulted for instance, currency experts (nāqid/sarrāf), for sorting out forged currency
2. Hand writing experts for recognizing writing in commercial transactions
3. Khāris; to access the quantity of grapes, dates, etc. while they were still in the tress.[314]

2.3.5.4.1 Physicians

Fiqh literature contains detailed discussions of specific injuries and the involvement of physicians in the process of determining retaliation or compensation for each of them. A partial list comprises the breaking or uprooting of a tooth, cutting of a finger, [315] different cuts on the skull, [316] and blows to the head that cause insanity or bring about a total or partial loss of sight, [317] hearing,[318] or speaking ability.

In was also permitted for the male physicians to teach females about how to treat other women. In case a female physician is not present and the life of a female patient is at risk only then a male practitioner is permitted to treat the patient. [319]

2.3.5.4.2 Slave Trade

---

[314] Sarakhsi, *al-Mabsūt*, vol. 23/ 5 &6, *Maūsūa Fiqhiyah al-Qūītīyah*, s.v. "Kharish" vol. 19, 101.
[315] *Al-Mughnī li-'Ibn-Qudāmah* 8/327 Ron Shaham, *Expert witness*, 72.
[316] Al-Shīrāzī, "Al-*Muhazab fī al-fiqh al-Imām Shafi'ī*", vol. 3/180, *Al-Mughnī li-'Ibn-Qudāmah* 8/321
[317] *Al-Mughnī li-'Ibn-Qudāmah* 8/329
[318] Ibid, 325, al-Shīrāzī, "Al-*Muhazab fī al-fiqh al-Imām Shafi'ī*", vol. 3/180.
[319] Sarakhsi, *al-Mabsūt*, vol. 10, 156.

One of commonest problems associated with the slave trade which necessitated the involvement of physicians was physical defects or diseases that a sale had before being transmitted to the unknowing buyer, who discovered them only after he took possession of the slave.[320]

2.3.5.4.3 Penal Laws

The opinion of experts was also required in realm of penal laws. Intentional physical offenses causing injuries may be established physically (Qiṣāṣ fima dun al-nafs), according to the Qur'ānic principle (5:45) of "an eye for an eye." This applies only to those cases in which the exacting of retaliation is possible i.e. where injury can be inflicted in exactly the same area, without risking the life of the offender and without causing graver harm than that inflicted on the offended person.[321]

2.3.5.4.4 Architects and Builders

In *Muqaddima, 'Ibn Khaldūn* (d. 1382) provides important information about the central role that construction experts played in medieval city life. He reports that in thickly populated cities, people quarrelled over internal and external space and over the use of the outer walls of buildings. [322] In these situations, role of experts essential to curb the disputes.

---

[320] *Maūsūa Fiqhiyah al-Qūītīyah*, s.v. "Khiyār al-'Aeb" vol. 20. 115.
[321] Ibn Rushd, "*Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*". 4/ 186.
[322] Ibn. Khaldūn, *The Muqaddimah: an introduction to history; vol. 2*. Trans. by Franz Rosenthal (New York: Pantheon Books, 1958), 361-362. Also in Shaham, Expert Testimony, 75.

2.3.5.4.5 Physical and Forensic Evidence

In penal laws, knowledgeable females (*Ahl Al-ma'rifa min al nisā'*) examine the women who have suffered physical damage to the private body parts and report about the severity of injuries and extent of a prerequisite of fixing amount of blood money (*Diyah*). [323]

It can be analysed here that Islamic law has always had the attitude of taking full benefit from the expert testimony. Today, if it is considered that a matter is beyond a layman's knowledge and wisdom, it is appropriate from the perspective of Islamic law to consult an expert and give the decision accordingly. However, authentication of an expert testimony is required by opinion of other experts as well.

2.3.6 Circumstantial Evidence (*Qarīna*)[324]

Most of the authorities, especially contemporary legal scholars, treat forensic evidence as a form of *qarīna* (circumstantial evidence).

Word Qarīna literally, means, in connection with, in conjunction with, and associated with. Judicially, it denotes any signs and indications which show the existence or non-existence of a fact in issue (the thing claimed),[325] and articulate its evidentiary value according to the rules that govern *qarīna*. For instance, al-Zuḥaīylī maintains:

> "As a matter of fact, on our contemporary time, there have emerged a number of powerful and clear forms of circumstantial evidences and indicators in the field of proof and evidence. For example, the identification of the culprit through fingerprints, blood testing, photographs, sound recordings, and blood sampling. . . .

[323] Ron Shaham, *Expert witness*, 96.
[324] On detailed discussion on circumstantial evidence in common law see Chap 3, sub topic 3.4.5.3
[325] Milton J. Cowan, *Dictionary of modern written Arabic*, 3rd ed., (Beirut: n.p, 1974), 760; Elias A. Elias, *Modern Dictionary: Arabic English* (Beirut: Dar al-Jalil, 1986), 537.

But the court has to be extremely cautious about using them as the chances of tampering with them are greatly worrisome."[326]

Prof. Anwārullah, another contemporary thinker, classifies a number of forensic processes as circumstantial evidence. These include, autopsy results on the corpse, blood spots, finger impression, footprints, identification by tracks, handwriting samples, injury marks, violence marks on private parts of body of victim, and presence of incriminating objects, like the weapon of the offence, and tire and radiator marks on the body of victim in case of accident.[327]

Another renowned expert in this field, Dābur, includes forensic evidence as *al qarā'in al-mustaḥdathah* (the modern types of circumstantial evidences). He points out that in case of an autopsy for determining death cause (for instance, when the criminal strangled the deceased and hanged him, just to show that the victim has committed suicide). Other examples include blood tests for identification purposes or verification of finger impression and foot-prints, found on the objects used in the killing. All the above-mentioned techniques, according to him, are all tools which makes the case stronger and a very strong source of authentication.[328]

Ibn Taīmīyyah, 'Ibn Qayīm al-Jawzīyyah and 'Ibn Farḥun integrated circumstantial evidence into fiqh doctrine of evidence and procedure. Ibn Qayīm went so far as stating that physical indicators are stronger evidence than the testimony of witnesses, because they do not lie. Expert witnesses, by knowing how to interpret physical indicators, or how to interpret "the language of things," become indispensable aids to judges.[329]

---

[326] Wahbah al-Zuhaīlī, *"Al-Fiqh al-Islamī wa 'Adiltuhu" vol6. (Damascus: Dār al-fikr,1985). 556.*
[327] Sikanadar Shah Ḥaneef. "Modern means of proof: Legal basis for its accommodation in Islamic law". 343.
[328] Ibid. 345.
[329] Shaham, *The expert witness*, 38.

2.3.6.1 Definition

Circumstantial Evidence in Islamic Law is lexically derived from the word *qarīna*. The word *qarīna* (pl. qarā'in) implies association, linkage, affiliation or genuine evidence. In the juristic sense, *qarīna* implies logical inference derived from certain facts from which a distinct conclusion can be reached at.[330]

Technically, the meaning of *qarīna* in Islamic Jurisprudence is "some set of information or facts which demonstrate the presence or non-presence of a thing (fact). The evidence of fact must be likely to be proved in the court."[331]

Ibn Qayīm was among the advocates of the utilization of *qarīna*. Indeed, even in *ḥudud* cases he stated that, "Whosoever refuses to apply *al-'Amarāt and al-'Alamāt (qarīna)* in Islamic law, verily, he has destroyed many rules and had neglected many rights." [332]

2.3.6.2 Legal Proofs from Qur'an

It is to be noted that this method of proof of evidence plays an essential role in some crimes in Islamic law. Majority of the scholars have accepted *qarīna* as a valid mean of proof. It is proper to quickly survey the affirmative evidence of *qarīna* in the *Qur'an*, *Sunnah*, and precedent of Companions of Prophet (PBUH). The evidence in *Qur'an* includes:

> "So they both raced each other to the door, and she tore his shirt form the back. They both found her lord near the door. She said: "What is the (fitting) punishment for one who formed an evil design against your wife, but prison or a grievous chastisement? He said: "It was she that sought to seduce me-from my (true)self" And one of her house hold saw (this) and bore witness, (thus)- "If it be that his shirt is rent from the

[330] Lisān al-'Arab, s.v "*Qarīna*", al-Misbāḥ al-Munīr, s.v "*Qarīna*".
[331] Muḥammad 'Amīm al-'Ihsān al-Mujaddadī al-Barkatī, *Qwā'id al-Fiqh*, vol. 1 (Karachi: Sadaf Publishers, 1986), 428.
[332] Muḥammad bin abī Bakr bin 'Ayūb ibn Qayīm al-Jaūziah, *Al-Turuq al-Ḥukmīyah* (Maktabah Dār al-Bayān, n.d), 4.

front, then her tale is true and he is a liar. But if it be that his shirt is torn from the back then she is the liar, and he is telling the truth!". So, when he saw his shirt that it was torn at the back- (Her husband) said: "Behold! It is a snare of you women. Truly, mighty is your snare!" O *Yūsuf*, pass this over! (O wife), ask forgiveness for your sin, for truly you are at a fault."[333]

These verses relate the tale of Prophet *Yūsuf* (Joseph) in the *Qur'an* and they are frequently cited in the fiqh books to legitimize the utilization of fortuitous proof in Islamic law. The charge of enticement against the youthful *Yūsuf* was ruled off through circumstantial evidence alone.

Another story in *Qur'an* regarding Prophet *Yūsuf* relates to the circumstantial evidence when his brothers hatched an evil plan against him:

"And (to substantiate their claim) they stained *Yūsuf*'s shirt with false blood. Their father (Prophet Yaqub) said "No, but your minds have made up a tale (that may pass) with you (for me) patience is most fitting; against that which you assert. It is God (alone) whose help can be sought!"[334]

According to Imām Al-Qurtubi, Muslim law specialists refer to this verse as direct authority for acceptance of a 'sign which demonstrates something' as a solution to problems as compurgation by Oath *(qasāmah)* and similar.[335] Muslim legal scholars believe that in spite of the false portrayal of *Yūsuf*'s siblings, the father Prophet Yaqūb knew from proof of truths that *Yūsuf* was not attacked by a wolf since his blood-stained shirt was not torn. This is a clear example of circumstantial evidence to decide the genuine way of issues when confronted with specific cases with a given set of facts. [336]

---

[333] Al-*Qur'an* [12:25-29]
[334] Al-*Qur'an* [12:18]
[335] 'Abu 'Abdullah bin 'Aḥmad bin 'Abi Bakr al-Qurṭubī. *Tafsīr Qurṭubī*. vol. 9, 2nd ed. (Cairo: Dār al-Kutub al-Miṣrīyah, 1964). 174.
[336] Ibid, vol. 9, 173.

2.3.6.3 Legal Proofs from Sunnah

Prophet (PBUH) also recognized circumstantial evidence as a mean of proof. He decided on the basis of circumstantial evidence in many cases. Prophet PBUH stated once:

> "There were two women who had small sons. A wolf came and took away the son of one of them; one of them said to other, "it was your son". The other said, "No, it was your son". They brought their dispute to Prophet Dāwūd A.S and he decided in favour of the elder. Then they went to Prophet Sulaīman A.S and related to him their dispute for decision. He ordered to provide him a knife to make two pieces of the child so as to give one piece to each one of them. On this the younger one of them said, "Don't cut him into pieces, this is the son of elder one". Hearing this Prophet Sulaīman (AS) decided in favor of the younger one."[337]

The above-mentioned narration of Prophet PBUH, narrates the importance of circumstantial evidence through the anecdote of Prophet Dāwūd and Prophet Sulaīman. A true mother refused to get the custody of child on the condition that her child should be alive. While the other women did not have that motherly affection with the baby that is why she agreed upon cutting of the baby. On that basis Prophet Sulaīman resolved the case. Prophet PBUH also decided cases of maternity of children, on the basis of *qiyāfah. Qiyāfah* is the procedure of defining paternity or nasab of a child on the basis of similarity of features and resemblance between one over another. This procedure is also called one of the process of circumstantial evidence or *Qarīna*.[338]

Caliph Umar ordered hadd punishment for a woman who was pregnant without marriage.[339]

---

[337] Muḥammad bin ʿIsmāīl ʾAbū ʿAbdullah al-bukhārī al-Jāfī, *Saḥīḥ al-Bukhāri*, vol.8 (Dār Ṭaūq al-najāt, n.d) bāb ʿizā Ida'at al-Mar'a ʾibnan, tradition no.6769, 156.

[338] Muhammad Munzil Muhammad et.all, "*Qarina*: Admissibility of Circumstantial Evidence in Ḥudud and Qaṣaṣ Cases", *Mediterranean Journal of Social Sciences* 2, vol.6 (2015) DOI: 10.5901/mjss. 2015.v6n2p141. https://www.researchgate.net/publication/273904870_Qarina_Admissibility_of_Circumstantial_Evidence_in_Hudud_and_Qisas_Cases. (accessed August 14, 2017)

[339] ʿAdnān Ḥassan ʿAzāīza, *Ḥujjīah al-Qarāi'n fī Sharī'ah al-Islāmiah al-basmāt - al-kiyāfah - dalalāt al-'asar-tehlīl al-dam* (Uman: Dār al-ʿAmār, 1989), 125.

Saḥiḥ Bukhārī quotes 'Ibn 'Abbās that he heard from 'Umar saying: I fear that a time would come when people would say that we do not find *ḥadd* of rajam in the book of Allah Almighty .... They will be misguided by not abiding by a duty. O Yes! Rajam is a duty upon who committed adultery and he was married if there is a proof, or pregnancy or confession.[340]

There is a difference of opinion among the scholars about whether *ḥadd* can be imposed on the basis of *Qarīna al-ḥabl* or not.

Imām *Abū Hanīfah* and Imām Shāfi'ī are of the view that it cannot if she refuses or stays quiet because there is no *ḥadd* punishment without proof or confession. She will not be stoned or lashed only on the basis of pregnancy. The circumstantial evidence must be authenticated or corroborated by others means as well. Like confession, or oral testimony, etc.[341]

There came a woman to 'Umar who was pregnant without husband. When 'Umar (God be pleased with him) asked her about it. She told him that she is a woman of deep sleep. She was sleeping and a man had sex with her. She said that when she woke up he was done with it. Umar after listening to the story took the orders of *ḥadd* punishment back due to the element of doubt in it.[342]

Circumstantial evidence has always been a strong mean of proof in the eyes of both law and Islamic law. There are two types of circumstantial evidence in Islamic law;

i) Strong Circumstantial Evidence *(Qarīna Qāti'ah)*

ii) Weak Circumstantial Evidence (*Qarīna Dha'īfah)*

---

[340] Muḥammad bin Isma'il . *Saḥiḥ al-Bukhari*, tradition no. 2829
[341] Al-Kasani, Al-Badai, vol. 7. 46.
[342] 'Adnān Ḥassan 'Azāīza, *Ḥujjīah al-Qarāi'n fi Sharī'ah al-Islāmiah*, 127

The strong circumstantial evidence are the ones which signifies strong belief and do not have the possibility of lies in it. Such types of circumstantial evidences are a strong source of proof in Islamic law and are advocated by *Qur'an* and *Sunnah.*

Weak circumstantial evidences are not admissible and they are not relied upon unless corroborated by other strong proofs.

2.3.6.4 Electronic Evidence

As far as the electronic evidence is concerned, there are two ways in which circumstantial evidence can be connected to it;

1. Electronic crime is proved with the help of physical circumstantial evidence. For instance, in a case *U.S v. Simpsons*, in which defended denied to accept that he was actually conversating with FBI agent in chat. The court did not accept the plea on the ground that the government officer authenticated this chat with him by way of a number of circumstantial evidences. Like, a piece of paper was found during the search of defendant on which street number, name and email address which was the same as given during the chat.[343]

2. Electronic Evidence is circumstantial evidence itself. Physical crime is proved with the help of circumstantial evidence which is electronic in nature. This can be best illustrated by case, in year 2012, a person named, Christian Aguilar disappeared. He was a friend of Pedro Bravo and both studied at the same University at Florida. Three weeks later, the dead body of Augilar, was found from a grave, 60 miles away from his residence. He was last seen with his friend Bravo. Police suspected Bravo had some relation with the disappearance. After search it was found that he was in possession of Augilar's backpack. The reason why Bravo was upset with Aguilar was

[343] United States v. Simpsons 152 F.3d 1241 (10th Cir 1998) [19]

that he had started a relationship with Bravo's ex-girlfriend. Hence, digital evidence made this circumstantial case far more certain. Electronic evidence experts had access to Bravo's cell phone and got many key pieces of proofs. Examiners found out that in the cache for the phone's Facebook app, there was a screen shot of a Siri search made near the time of Aguilar's disappearance that read, "I need to hide my roommate." Determining the tower that received signals from the cell phone, showed that Bravo had moved far to the west after the disappearance. In the end, examiners were able to investigate that the flashlight app on the cell phone was used for almost one hour after the disappearance. After these evidences and proofs, Bravo was tried in the court, in August 2014. During cross examination he admitted the crime and was convicted of first-degree murder. [344]

The matters in which electronic evidence is the proof itself as a circumstantial evidence to the case, electronic evidence is considered as a very strong proof. These proofs are a centre of attraction for the investigation officers because these proofs cannot be denied. For instance, DNA test, finger prints, call records, text messages (record of the numbers and timings and on which texts are sent). These are the proofs which cannot be denied by the criminals themselves unless backed by a very strong evidence.

If the nature of the evidence is such that it does not involve human intervention and the system through which it is generated is reliable, then such evidence is a strong evidence. The

[344] Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, "Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence" Rand Cooperation, 2015, 3. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf. (accessed, May 9, 2017) Also in, Dan Morse, Philip Welsh's simple life hampers search for his killer, Washington Post, May 6, 2014 https://www.washingtonpost.com/local/crime/philip-welshs-simple-life-hampers-search-for-his-killer/2014/05/05/1fd20a52-cff7-11e3-a6b1-45c4dffb85a6_story.html?utm_term=.cc88146e147f

evidence serves as a circumstantial evidence to the crime taken place in the physical world, such as murder, robbery or terrorism. Such crimes are committed through the help of electronic means. The suspects' calls are traced; their laptops are seized which can result in the investigation of number of clues. All of these are circumstantial evidence and play an integral role in investigation. [345]

It is proved that circumstantial evidence has great importance in proving and disproving electronic evidence. Islamic law has relied greatly on circumstantial evidence. *Qur'an*, *Sunnah* and conduct of Companions of Prophet (PBUH) have relied heavily on strong circumstantial evidence (which are beyond doubt). So, it is automatically proved that electronic evidences for cyber-crime, which are beyond doubt, would be acceptable in Islamic law and such evidence would be binding in nature. But it must be ensured that nature of e-evidence must be free of all types of doubts, alterations or errors.

2.4 Conclusion

Islamic law of evidence is a very compact, fool proof and universal in nature. It has covered almost all the areas of evidence which are discussed in today's world. Ranging from oral testimony to documentary evidence, expert testimony to circumstantial evidence. Islamic law of evidence has covered all the means of proofs which are sought in modern trials.

Evidence in Islamic law is correctly denoted by the term "bayyinah" which means proof. There are seven means of proof in Islamic law. It includes confession, oath, testimony, documentary evidence, expert testimony, circumstantial evidence and knowledge of the judge.

[345] Danial J. Lynch and Ian Brenson, "Computer Generated Evidence: The Impact of Computer Technology on the Traditional Rules of Evidence." *Loy. U. Chi. LJ* 20 (1988): 919.

All the means of proofs are covered in great detail leaving no room for ambiguities for today's problems. All the means are well-elaborated from all perspectives which makes it easier to analyse how those laws would be applicable in today's world.

In this chapter, oral testimony, documentary evidence, expert testimony and circumstantial evidence were discussed at length because of having relatively closer link with electronic evidence.

Islamic law presents special precautions for oral testimony as compared to western law. Oral testimony is a back bone of Islamic law of evidence. Islamic law ensures that if the character of the witness is doubtful then his or her testimony is inadmissible. A special process of purgation is present in Islamic law where the witnesses are passed through the process of screening in terms of their character. The judges check the character of witness, either good or bad. This ultimately makes it easier for the judge to decide that whether this person is honest enough to testify about the rights of other people or not.

Islamic law puts different kinds of limitations on oral testimony. For instance, father cannot testify for son and vice versa. Sisters cannot testify for brother and wife and husband cannot testify for each other, etc. There are no such restrictions in western law.

Broadly there are two categories for conditions for testimony. One of them are condition of bearing of testimony (Shurut at-Taḥamul) which includes conditions such as sanity, sightedness, puberty and direct observation of witness.

Other category is about conditions of performance (Shurūt al-Adā). According to these, a witness must be a Muslim, free and adult. He must have good memory, understanding and a just character ('Ādil), etc.

The concept of hearsay is also different in Islamic law. Hearsay is allowed only in few cases, which are not even hearsay in the technical sense. The reason being, Islamic law allows only those cases of hearsay which are famous on the basis of public knowledge. These cases include: birth, marriage, death, etc. This concept is called Shahāda bi-Tasāmay'.

A concept of secondary witness is allowed in Islamic law. There are cases when witness cannot come to the court, probably because he died or is on death bed, or he is out of city. In these cases, he will make another just witness his representative and send him to the court to testify. This concept is called *Shahādah* 'ala *shahādah.*

Due to the shift in technology, common law has shifted its reliance more on circumstantial evidence, documentary evidence, and expert testimony. Common law relies more on the evidence in which human input is not present. In this age, machines are relied more than humans. For instance, computer generated records.[346]

Today, there is a dire need for a research which sheds light on the admissibility of electronic evidence in Islamic law through modern means of proofs. There is no doubt that Islamic law address these modern means of proof directly but detailed analysis and deep research shows that Islamic law does address these issues. Because, no case is possible without involvement of these evidence. Almost one third of the law suits involve electronic evidence. Secondly, on one side, as humans have started relying more on electronic evidence, there are also human minds who are busy misusing technology. Cybercrimes have increased considerably during the last few years. That is why safeguard needs to be prepared. Scholars of Islamic law cannot be silent on these areas anymore. Principles in Islamic law are present but there is a dire need to elaborate them in the light of Shariah.

---

[346] These are those type of evidence is considered as strongest documentary evidence. it includes call logs, ATM machines records, timings or bank statements. There are hundreds of such examples which are relied much in courts, other than humans' statements. Statements are admissible subject to corroboration with other circumstantial evidence.

Documentary evidence is also being heavily relied upon nowadays in civil suits, which are mostly computer-generated records.

Similarly, today's reliance of court system on expert witness has increased a lot after the advent of electronic evidence. Books of Islamic jurisprudence are filled with hundreds of such examples when the judge of the court used to take help from experts of different fields in the matters which were beyond humans reasoning. Jurists however differ on the opinion that how many of the witness are required in order to authenticate. But it is unanimously agreed that expert testimony is admissible. [347] Circumstantial evidence is also one of the most popular means of proof in case of electronic evidence. Same was the case in classical Islamic law cases. Even *Qur'an* at so many places teaches us to decide the cases on the basis of circumstantial evidence.

Even the objectives of Shar'īah (Maqasid al- Shar'īah) and legal maxims in Islamic law prove that something which is so essential for the administration of justice and management of human needs, that cannot be avoided, should not be avoided if it is not infringing the rulings of Sharī'ah.

It is an established fact that electronic evidence assists in administration of public and private institution and it assists in meeting the ends of justice. It does not hinder the administration of justice. Secondly, the crimes taking place in cyber world cannot be avoided and they need to be stopped. There are five objectives of Shariah. Among them are protection of money, protection of life. For ensuring objectives of Shariah, electronic evidence need to be recognized and admitted.

---

[347] *Imām Abū Ḥanīfa* mentions in few cases that witness must be God fearing in matters related to rituals such as is a woman is lactating mother and she fears that fasting would put negative effect on her health, in this case *Imām Abū Ḥanīfa* says, she should consult a God-fearing physician.

According to the latest statistics, the banks and financial institutions are the biggest targets of hackers who steal millions of dollars yearly. [348] So, curbing that is a necessary requirement for fulfilling the objectives of Sharī'ah.

Similarly, cyber terrorism is spreading at a high speed. It is the cause of destruction of many human lives. So, proper measure of cyber security and proper legislation for executing cyber criminals is a necessary element to meet the first objective of Sharī'ah.

[348] Alexander Jones. Cyber Crime: The Growing Threat to Global Banking. International Banker. Nov 30. 2016. **https://internationalbanker.com/banking/cybercrime-growing-threat-global-banking/** (Accessed: May 9. 2018)

CHAPTER 3 ADMISSIBILITY OF ELECTRONIC EVIDENCE: THE INITIAL STAGE

3.1 Introduction

Having the lengthiest practical experience of almost 1100 years, Islamic law of evidence is without doubt the most established and fool proof legal system. The means of proof in Islamic law of evidence are oral testimony, documentary evidence, circumstantial evidence, etc. All these means have a link with electronic evidence as well.

English law on the other hand, evolved much later than Islamic law. There are a number of things which are common in the English and Islamic laws. Researching both the laws, it would not be incorrect to state that the basic structure of both Islamic and English law is the same. For the current research, US law is chosen for further research on electronic evidence. Examples of other countries are quoted where required.

The admissibility of physical as well as electronic evidence in the U.S law is dependent on four steps, agreed upon by the legal experts;

1. Relevance
2. Authentication
3. Hearsay rule
4. Best evidence rule

This chapter and next two chapters are devoted to discuss the three stages of electronic evidence in the western legal system; "initial stage of electronic evidence", "the subsequent stage" and "the trial stage"

3.2 Initial Stage of Admissibility

The initial stage of admissibility of electronic evidence comprises of relevance and authentication.

One of the leading Judgments on admissibility of electronic evidence is Lorraine v. Markel American Ins. Co.[349] Judge Grimm stated that the proponent must overcome four hurdles to let the evidence be admissible in the court of law. Judgment states as follows:

> "Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant...(does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant.., is it authentic...(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay..., and if so, is it covered by an applicable exception ....; (4) is the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, of if not, is there admissible secondary evidence to prove the content of the ESI...; and by the courts" [350]

It means that the document should be reliable, accurate and trustworthy. It must be subjected to proof of integrity, provenance and chain of custody.[351]

3.3 Relevance

Relevance is a matter of appreciation by the Judge. The relevance is usually defined as, 'any two facts to which it is applied are so related to each other that according to the common course of events one either taken by itself or in connection with other facts proves or renders probable the past, present or future existence or non-existence of the other'.[352]

---

[349] 241 F.R.D. 534 (D. Md. 2007)

[350] Ibid, 12.

[351] Chain of custody means the document must be present in reliable custody. It contains a chain which proofs that at no time, the record or data was left in an unreliable custody which could tampered or affect the integrity of that evidence.

[352] Olivier Leroux, Legal Admissibility of electronic evidence, *International Review of Law, Computers & Technology* 18, no. 2(2007), 198.

Evidence is relevant if it has the tendency of making the existence of any fact 'more or less probable'. It means that if it is logically probative or disapprobative of the matter which requires proof. It is the matter of a common sense and experience.[353]

There is a distinction between the admissibility of evidence and the weight to which it is entitled in the eyes of fact finder. It is not necessary that evidence should carry weight in order to be relevant. It is sufficient if it has any tendency to prove or disprove a consequential fact in the litigation.[354]

Those facts from which existence or non-existence of a fact in issue may be inferred are also relevant. They are also called 'fact relevant to the issue' or 'evidentiary fact'. If only facts in issue are open to proof or disproof, many claims and defences would fail. Quite often, the available facts are only those which can establish some other facts or facts relevant to the facts in issue. [355]

The relevance of the evidence is decided by the judge based on his own discretion, when brought to him by the parties. There is no strict or rigid legal rule of evidence and as the judicial system is mainly based on accusatorial mechanism, English judges can freely appreciate the relevance of the proofs. When the evidence has shown to meet the low threshold of relevance, it has a presumption of admissibility unless it is excluded by statute, rule of evidence or procedure, or constitution. [356]

---

[353]Ibid.

[354] David Faigman, "Evidence: Admissibility vs. Weight in Scientific Testimony." *The Judges' Book* 1, no. 1 (2017): 11.

[355] Olivier Leroux, Legal Admissibility of electronic evidence, 198.

[356] Jon. R. Waltz, "Judicial Discretion in the Admission of Evidence under the Federal Rules of Evidence." *Nw. UL Rev* .79 (1984): 1097.

Once the evidence is deemed relevant, it is "weighted". Weighing involves scrutiny of evidence that is which evidence is acceptable and which is to be rejected. Law of evidence generally is clear that the evidence is inadmissible if it is not relevant.[357]

3.4 Authentication

Once it is established that the evidence is relevant, the next step on which the lawyer is supposed to satisfy the judge is that the evidence is authentic. This is the characteristic which is very important for admissibility of electronic evidence. [358]

Authentication of physical evidence is also mandatory but the rule and principles are established. The existence of e-evidence in many forms gives rise to a number of problems especially when it comes to authentication of e-evidence. For instance, data files, meta data, emails, text messages, log files, mobile calls, etc. All these types require different technique of authentication. This chapter will discuss with an example, the authentication of emails, websites and instant messages. Due to space constraints, inclusion of all authentication means is not possible, but the two main technologies that are generally used in authentication shall be discussed; hash tagging and Meta data.[359]

Condition of authentication for electronic evidence is necessary. It must be beyond reasonable doubt, and excludes unreliable information. The evidence must be offered in a form which is, "sufficient to support a finding that the matter in question is what its proponent claims."[360]

This stage is probably the most important because it serves as a foundation of trust of judges. If there are doubts about the authentication, it renders the evidence inadmissible.

---

[357] *Lorraine v. Markel.* 241 F.R.D. 534 (D. Md. 2007), 14.
[358] Ibid, 16.
[359] Mason, *Electronic Evidence*, 254.
[360] Nathan Judish, ed. *Searching and seizing computers and obtaining electronic evidence in criminal investigations* (Office of Legal Education, Executive Office for United States Attorneys, 2009), 197.

These issues can be resolved if the parties employ proper procedures to preserve and identify ESI. Documenting the chain of custody during the production process is also very important. But it must be anticipated that not all the parties will have the procedures rightly placed. So there may be disputes regarding the authenticity of documents.

The digital information lacks physical appearances and creates many doubts about the actual sender or the creator of the document. These issues are heightened when hacking takes place against various accounts/email addresses. Anyone can send a message from someone's mobile phone. So, the issue arises as to how the true sender would be authenticated. As anyone can alter the data displayed on the internet or websites, it is a challenge for the proponent to prove the authenticity of certain documents.

Due to the difference in types of electronic data, authentication techniques vary according to the nature of a file or a document. In other words, the difference in the nature of electronic files changes the evidential foundation of such documents, e.g. emails, websites, instant messaging, electronic contracts. Other types include, authentication of hard drives, data storage devices like USB's, etc. Some cases may involve authentication of material from a database. Information from database is entirely a different type of data and files, and are dealt differently in the courts.

Provenance and chain of custody is mandatory to be proved in court for authentication. This fragile nature of data changes very rapidly which raises concerns regarding the integrity of the document.

The upcoming sections will discuss the issues of authentication and propose corresponding solutions.

3.4.1 Definition

The term 'authentic' is used to judge whether the data or a document is genuine, or that the document 'matches the claims made about it'. As already stated, electronic data is not restricted to simple text documents. The format of data can be of a more technical nature. For example, where active components such as macros and scripting language are involved in the data, it results in more complex interpretation of the text to make it readable.[361] The nature and characteristics of electronic document reveals that if files are displayed on a different computer, other than the one originated, it may result in change of font and different line breaks. [362] This results in the creation of new Meta data and affects its reliability scale. Another issue that arises in these cases pertains to identify the exact document from the mentioned documents which is original and final. These differences put jurors in a fix to design some more compact and fool proof standards to authenticate documents.

The definition of authenticity in terms of a physical document comprises of attributes as state of being the original, or more appropriately, of being faithful to an original, uncorrupted and probably with a verified provenance[363]. The standards of authentication for digital objects must fulfil the same criteria.

3.4.3 Common Challenges

A number of challenges are confronted when dealing with electronic evidence which include:

a) A claim that the electronic data is damaged, changed or manipulated during the time it was created and the time it was presented before the court.

[361] Stephen Mason et al., *Electronic Evidence* 2nd edition (Haryana: LexisNexis, 2012), 109.
[362] Ibid. Also in, *Searching and Seizing Computers*, 197.
[363] It means the document must be comprised of the attributes such as unique, unambiguous, concise, repeatable and comprehensible.

b) The computer programme which generated the record may be doubtful from reliability point of view.

c) The author may be disputed. For example, the person responsible for writing an email or a message may refuse that they wrote the text, or sufficient evidence is not present to adduce the nexus between the evidence and the person responsible for writing the communication.

d) Reliability from the social networking website may be disputed.

e) There might be a dispute about the person who alleged to have used the pin, password or clicked the icon "I accept" is the actual person who carried out the action. Whether the person alleged to have used their PIN, password or clicked the 'I accept' icon was the person that actually carried out the action.[364]

In this aspect, digital data has a capacity of proving considerably negative as observed by Prof Tapper.[365] He gave an example of Application Transaction Counter on the chip on a debit card. Another case maybe when a number of clients report about illegal withdrawal of money from the ATM's which instigates the banking authorities to investigate whether an employee is behind the theft. For instance, in the case *U.S v. Bonallo*[366], in which the records of the bank showed that the cash withdrawals took place when Bonallo was present in the building. It was assumed by the employees that Bonallo's duties after his employment terminated discovered a fraud program in the PC of Bonallo. That program was designed to give access to ATM computer file. Although it could be utilized for a legal objective. [367]

---

[364] Ibid, 112.
[365] Daniel K. B. Seng, "Computer output as evidence", *Singapore Journal of Legal Studies* (1977), pp 163- 169.
[366] United States of America v Bonallo, 858 F.2d 1427 (9th Cir. 1988)
[367] Ibid. Mason, Electronic Evidence, 226.

3.4.3.1 Alterations

Opposing parties often allege that computer records lack authenticity because electronic records can be altered easily. Or they often challenge on the ground that the documents have been tampered with or changed after they were created. Nowadays, courts have generally rejected arguments that electronic evidence is "inherently unreliable" for having a potential for manipulation. In case of paper documents, the mere possibility of alteration is not sufficient to exclude the evidence. Similar is the case with electronic evidence. Absence of specific evidence of alteration, the evidence of weight is affected and not the admissibility. In case of *United States v. Safavian,*[368] and *United States v. Whitaker,*[369] the court observed that "The fact that it is possible to alter the data contained in a computer is plainly insufficient to establish untrustworthiness". Similarly, in case, *United States v. Glasser,*[370] the court commented that, "The existence of an airtight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."

3.4.3.2 Authorship

In case of handwritten documents, there is a confusion that they may be written in different handwriting style, date stored on computer does not necessarily identify the author. This is an actual problem with electronic communications, which put the authors in unusual anonymity. For instance, Internet technologies allow their users to send anonymous emails,

---

[368] *US v. Safavian,* 435 F. Supp. 2d 36, 41 (D.D.C. 2006).
https://casetext.com/case/us-v-safavian-4
[369] US V Whitaker, 127 F.3d 595, 602 (7th Cir. 1997).
https://casetext.com/search?q=127%20F.3d%20595,%20602%20(7th%20Cir.%201997
[370] United States v. Glasser, 7173 F.2d 1553, 1559 (11th Cir. 1985),
https://casetext.com/search?q=773%20F.2d%201553,%201559%20(11th%20Cir.%201985)

and Internet Relay Chat channels allow the authors to chat without revealing their real identity. When such computer stored communication is admitted in the case, the defendant party may take the defence by challenging the authenticity by putting identity of author in doubt. In these cases, circumstantial evidence helps a lot in proving or disproving the authorship of a computer-stored data.[371] Distinctive characteristics such as email addresses, nicknames, signature blocks, and message contents can prove authorship, at least sufficient to meet the threshold for authenticity. [372]

3.4.4 Electronic Data Classification

To establish evidential foundation of digital evidence during trial, it has to be proved that the document is what it claims to be. The authenticity of digital evidence may be challenging because it has very different characteristics as compared to paper evidence. Rules developed for physical and documentary evidence are applied to electronic evidence.[373]

In order to cope with different challenges of authentication, scholars and judges have classified electronic data into different categories. These classifications are very helpful when authentication of data is required. Primarily these categories are based on degree of human input involved in electronic data. The categories are:

3.4.4.1 Computer Stored Data

The records of activities that involve the written content by one or more people. For example, emails, word processing files and messages. From the evidential point of

[371] United States v. Simpsons 152 F.3d 1241 (10th Cir 1998) [19]
[372] Ibid.
[373] Orin S. Kerr, "Digital evidence and the new criminal procedure." *Colum. L. Rev.* 105 (2005): 279.

view, it would be necessary to establish that the content of the document is a reliable record of human statement.[374]

3.4.4.2 Computer Generated Data

Records generated by computer that does not involve human intervention. Examples of these types of records are data logs, telephone connections, and ATM transactions. The main evidential problem with this type of records is to establish that the computer program was working properly at that time.[375]

3.4.4.3 Computer Generated and Stored Data

Records consisting of a mix of both human input and calculations generated and stored by a computer. Example of this type may be of spread sheet that contain human statements (input to the spreadsheet program), and computer processing (mathematical calculations performed by the spreadsheet program). The evidential issue here would be, whether the person or the computer created the record. Another issue could be regarding how much of the content was created by the computer and how much by the human being. It may be possible that human input could be hearsay or the authenticity of the computer processing might be an issue.[376]

In *Elf Caledona Ltd v. London Bridge Engineering Ltd*[377], Lord Caplan noted the following observations regarding the categories of evidence:

> "The defenders suggested that there are three categories of use for computers. They can be used to record data without the need of human intervention. The Spectra-Tek program was described as being of this type. It was said that what this program prints out may be regarded as real evidence. However, Counsel had to concede that even this type of computer exercise

[374] A. Comment, A Reconsideration of the Admissibility of Computer-Generated Evidence, 126 U. PA. L. Rev. 425 (1977). Jerome J. Roberts, "A Practitioner's Primer on Computer-Generated Evidence." *The University of Chicago Law Review* 41, no. 2 (1974): 254-280.
[375] Ibid.
[376] Stephen Mason, *Electronic Evidence*, 109.
[377] [2000] Lloyd's Rep IR 249

depends on the reliability of the program material. Unless it is properly programmed it will not store and regurgitate facts accurately. ...

Another category of computer use was said to be where the data is recorded by the computer and the data is put in manually. Thus, Piper would regularly send information to the beach and this would be entered in the computer system. It was accepted that to prove this material would involve some hearsay evidence unless the persons who entered the material in the computer were led as witnesses. However, the defender did not explore just what evidence would be required in the situations under consideration. In general, it seems to me that here must be many cases where it would not be practicable to lead the person who generated the data and the person who fed it into the computer so that there must be some practical limits as to what proof can be expected in this kind of computer evidence.

It was submitted that the third type of computer situation is where the computer is used by experts to carry out calculations or simulations. It was claimed that in this kind of situation the general rules relating to expert evidence should be applied. Certainly, in this kind of situation, one can get a distorted result if one factor is in-putted wrongly. The kind of the computer models used by expert, of course, generally requires more than normal discrimination and judgment in the selection of input material. Thus, the expert will have to prove how the input material arrived at and the justification for selecting what was put in."

3.4.4.4. Authentication Requirements

Both the computer stored and computer-generated records have some standard requirements to be authenticated. This section briefly discusses the basic requirements.

3.4.4.4.1 Computer Stored Data

The standard for authenticating computer records is the same as that for authenticating other records. Although some litigants have argued for more stringent authenticity standards for electronic evidence, courts have resisted those arguments.[378] In case *re F.P.*[379], it was held that..."We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity".

---

[378] See, e.g., *United States v. Simpson*, 152 F.3d 1241, 1249-50 (10th Cir. 1998) (applying general rule. standard to transcript of chat room discussions)

[379] 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005)

Computer stored records involve human input and statements. That is why their authentication involves proof of the reliability upon the statement. Oral testimony is the first tool in authentication of such documents.

Other methods for authentication of computer stored information include, "authentication by circumstantial evidence". This method is very useful in case of authentication of instant messages, emails, and social networking web posts, etc. These methods are further elaborated in the upcoming section.[380]

3.4.4.4.2 Computer Generated Evidence

These documents are not subjected by law to pass the strict levels of admissibility.

Computer stored evidence requires oral testimony regarding the authenticity of the document's content and the document itself. But this is not the case in computer generated records. Many judges have considered it as frivolous to reject evidence solely on the ground of that how the electronic evidence is generated. It was observed that call records are automatically generated and are retained in ordinary course of business. So these evidence are reliable almost every where around the globe for instance, federal rules of evidence.[381]

Since computer generated records are generated automatically so it is not necessary to prove that the witness has personal knowledge of the creator of data. Proof of the safe custody and proper methods used for preservation of data would be enough to authenticate. In *Lorrain v. Markel*[382], it was observed that it is not required that the authentication witness have

[380] *United State v. Tank* 200 F.3d 627 (9th Cir. 2000). *US v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000)
[381] Stephen Mason, Electronic Evidence, 485.
[382] 241 F.R.D. 534 (D. Md. 2007).

personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made.[383]

In case of business records, even if the witness is not personally familiar with some specific computer exhibits offered as evidence, they can be accepted. The most important thing is that the witness is in a position to testify that the business organization is relying on such record in order to run the business. Such reliance records in order to run their day to day business develops a level of trust. It is not the requirement that the witness is sufficiently equipped with the technical information of the records.[384]

3.4.5 Authentication Methods

Oral testimony, expert testimony and circumstantial evidence are the most significant tools for authentication of electronic evidence. This section discusses the different methods and the technologies involved for authentication of electronic evidence.

3.4.5.1 Oral Testimony

Generally, courts have considered oral testimony essential for authentication of electronic evidence. It means that the witness testifies for having personal knowledge about the evidence. Like, in case of *United states v. Kassimu*, the court observed that the copies generated by a computer of railway station office, can only be authenticated by the person who keeps the custodian or anyone who has personal knowledge about how the record is generated.

---

[383] Ibid, 23

[384] R v Lemay (2004) 227 WA 247

It is not a necessary condition that a person who has personal knowledge must be a computer expert. There is no compulsion that the witness must have programmed the computer or must have the knowledge of operations of computer. He must have actively participated in keeping the records or observe how they are kept.

For instance, in *St. Luke's*[385] case it was decided by the court that in order to authenticate printouts from a website, the party offering the evidence must produce some affidavit or statement from a person with knowledge (of website) such as a webmaster or someone else with personal knowledge. In this case, the court excluded the computer exhibits as evidence because affidavits used for authentication were factually inaccurate and affiants lacked personal knowledge of facts. The printouts of any electronic records or data are admissible when subjected to the testimony of witnesses or proper proof of reliability of such documents.

Courts do not accept the oral evidence or the paper printout of computer exhibits where the witness cannot testify by his own knowledge that so and so evidence is reliable and handled in the due course of business. The same situation was faced in the case *Harper*[386], when the appellant presented a Capital Card during travelling on a London Transport bus. A revenue inspection protection officer identified the number as one noted on a list of cards that had been stolen. The prosecution had to prove that the card was stolen. The judge rejected the evidence on the ground that the witness could not from his own knowledge testify the reliability of computer.[387]

Requirement of personal knowledge by the witness is relevant when the data is dependent on human input. But when the data is purely automated, i.e. complete production

---

[385] St. Luke's Cataract and Laser Institute PA v. Sanderson, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006
[386] R v Harper [1989] 2 All ER 208, [1989] 1 WLR 441 at 443. R v Minors (Craig).
[387] Ibid.

of computer without human input, the testimony of witness shifts to the integrity of the system.[388]

3.4.5.2 Expert Testimony

Expert testimony is taken where there is a matter of technical nature. The matter which is beyond the understanding of a layman is referred to as expert witness. Field of electronic evidence is intertwined with legal as well as technical matters.

It depends on the nature of the case. But the issue regarding the criteria of the qualification of an expert, may arise in cases involving electronic evidence. As the opposing party may challenge the authority of the expert witness, in that case the court would decide whether the person can qualify as an expert or not. [389]

3.4.5.2.1 Qualification of Expert Witness

Presence of expert testimony in any case is decided by the judge. There are a number of judicial opinions present on this matter. It is the preliminary matter for the judge to decide about the competency of the judge, not expanding the satellite litigations finding the competency of experts. [390]

---

[388] This issue is discussed in detail in 4.2.3.1(business record section).

[389] *Frye v. United States*, 54 App. D. C. 46, 293 F. 1013 (1923). *Daubert v. Merrell Dow Pharmaceuticals*, Inc., 509 U. S. 579, 589

[390] *R v Oakley* (2010) EWCA Crim. 2419. *R v. Coultas* [2002] WASCA 131. *Frye v. United States*, 54 App. D. C. 46, 293 F. 1013 (1923). *Daubert v. Merrell Dow Pharmaceuticals*, Inc., 509 U. S. 579, 589. Also, in Mason, *Electronic Evidence, 486*

UK's Perspective on Expert Testimony

The test of admissibility of expert opinion generally followed in England is discussed by King CJ in the case *R v Bonython*[391]. The South Australian Supreme Court concluded there were two tests for the trial judge to decide:

> "(a) whether the subject matter of the opinion is such that a person without instruction or experience in the area of knowledge or human experience would be able to form a sound judgment on the matter without the assistance of witnesses possession special knowledge or experience in the area, and (b) whether the subject matter of the opinion forms part of a body of knowledge or experience which is sufficiently organized or recognized to be accepted as a reliable body of knowledge or experience, a special acquaintance with which by the witness would render his opinion of assistance to the court. The second question is whether the witness has acquired by study or experience sufficient knowledge of the subject to render his opinion of value in resolving the issues before the court."[392]

There are two aspects which need to be kept in mind; do the expert carry any special qualification or experience regarding the relevant area? Whether his opinion is acceptable because of some other incentive. If an expert is not carrying any special experience, then weight of his testimony will be affected rather than admissibility.[393]

It is also acceptable that a person testifying carries some special experience other than relevant knowledge about it. Like in case *R v Oakley*, [394] one of the police officers testified regarding a road accident. His opinion was accepted because he had 15 years' experience in the field of traffic division and he had attended more than 400 fatal road accidents. But it is

---

[391] http://www.civiljustice.gov.hk/fr/paperhtml/fr374.html (1984) 15 SASR 364, 366

[392] [1984] SASR 45 at 46-47.

[393] 1. R v Silver lock [1894] 2 QB 766 (handwriting compared by a police superintendent); R v Somers [1963] 3 All ER 808, [1963] 1 WLR 1306, CA (medical doctor interpreting a report); R v Davis [1962] 3 All ER 97, [1962] 1 WLR 1111, CMAC (a witness can state the impression they formed as to the condition of the accused at the time they saw the accused).

[394] (2010) EWCA Crim 2419.

not the case every time, like in case *R v. Coultas*, [395] court rejected the opinion of a police officer who did forensic examination of a mobile phone.

3.4.5.3 Circumstantial Evidence

Due to the complexity in nature of electronic evidence, the courts usually consider a variety of means to prove or authenticate electronic evidence. For instance, the court will consider expert or non-expert oral testimony or some other hints or clues pointing towards the truth. It is called circumstantial evidence. Nowadays, circumstantial evidence is serving to be one of the most reliable and authentic proof of evidence. [396] Circumstantial evidence is drawn out of indirect observations related to fact in issue.[397]

The concept that the accused cannot be convicted merely on the basic of circumstantial evidence is wrong. Most of the criminal punishments are based on circumstantial evidence. In *U.S v. Simpsons*, [398] it was objected by the defendant that the conversation alleged to be originated from him is not actually his. Plea of the defendant was rejected on the basis of circumstantial evidence. The defendant gave a phone number, email and address to the FBI agent during chat. The same was seized from his computer table of during search operation.

In this case, *US v. Siddiqui*[399], a series of emails were put forward by the government as evidence and it was claimed that the defendant purportedly sent them to third party witnesses. The recipients testified that they received the emails. The defendant refused to admit that he was the sender of those emails. He argued that the government failed to prove him being the one who sent those emails. However, each email carried the defendant's e-mail

---

[395] [2002] WASCA 131.
[396] Orin S. Kerr, Computer Records and the Federal Rules of Evidence, (2001). US Department of Justice, 18.
[397] Encyclopaedia of Britannica s. v 'circumstantial evidence'. www.britanica.com/topic/circumstantial-evidence (accessed: May 13, 17)
[398] 252 U.S. 465 (40 S.Ct. 364, 64 L.Ed. 665)
[399] 235 F.3d 1318, 1322-23 (11th Cir. 2000)

address. One of the recipients of the emails testified that when he clicked on "reply" to the email, his mailing system displayed the defendant's email address. The emails carried the content in which the sender wrote about the details of the defendant's illegal conduct and referred to the author as "Mo" which was a nickname for the defendant. Finally, the recipients also testified that they spoke by phone with the defendant shortly after receiving the emails and in those conversations, he repeated the content of the email. The court held that these circumstantial evidences are sufficient to authenticate the emails.

A case titled, *Public Prosecutor v. Neo Khoon Sing*,[400] the judgment was taken solely on the basis of circumstantial evidence. The facts of the case are that the accused worked at National Environment Agency North-East Regional Office (NEA NERO). He sent two false terrorist attack warning messages through the website of Ministry of Home Affairs. He later on sent a third alarming message through the website of the Prime Minister's office. Later on, the police revealed that the messages emanated from the NEA's computer network. In fact, they were sent from the desktop computer located in the office in which the accused worked and was allocated for use to the accused. The accused claimed defence of alibi, and also claimed that it was probably done by an imposter who had access to his computer. He called digital evidence specialist to support this theory.

The digital evidence demonstrated that exactly 29 minutes after sending the first alarming message, the office computer was used to log on to the account of the accused. Same happened after sending the second message. It was further revealed that after sending the emails, the online government directory was seen by the recipient's address from the same computer. Also, exactly 10 minutes later, a work-related email was sent. The timing of sending those threatening messages and logging into the account of the accused contradicted

[400] [2008] SGDC 225.

that he was absent from the office. Additionally, the accused admitted on cross examination that it was not possible for any stranger to have access to his office. Hence the decision was made against him.

Another case, *Sunny Ang. v. PP*[401] was decided on the basis of circumstantial evidence. The following explains what was observed in this case with regards to circumstantial evidence:

> "The Sunny Ang test arose out of the following direction the trial judge gave to the jury in his summing-up at the close of the case: "Now, as I told you earlier on, one of the points about circumstantial evidence is its cumulative effect. Any one of these points taken alone might, you may think, be capable of explanation. The question for you is: where does the totality of them, the total effect of them, all lead you to? Adding them together, considering them, not merely each one in itself, but altogether, does it or does it not lead you to the irresistible inference and conclusion that the accused committed this crime? Or is there some other reasonably possible explanation of those facts?" The prosecution case is that the effect of all this evidence drives you inevitably and inexorably to the one conclusion and one conclusion only: that it was the accused who intentionally caused the death of this young girl."

3.4.5.4 Hash Value

Hash Values have a huge importance especially in digital forensics. Hash values are principally used for verification of digital data. These values are generated from a document, at the start of the investigation, which makes the integrity of digital material verifiable. Later, at the time of delivering document the hash values are compared to initial ones. It discloses if the documents is tampered or not.[402] Another very important use of hash values is identification and classification of document. Electronic documents are saved in many copies and in many places. [403]

---

[401] [1967] 2 MLJ 195.

[402] Netherlands Forensic Institute, forensic use of Hash Values and Associated Hash Algorithms, January 2018, 2. Available at: https://www.forensischinstituut.nl/binaries/nfi/documenten/publicaties/2018/02/13/vakbijlage-forensisch-gebruik-van-bestandskenmerken-en-bijbehorende-hashalgoritmen/Supplement-hashes-v2018_01a_English.pdf. (Last Accessed June 25, 2019)

[403] Ibid, 4.

It means "A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values, so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production." [404]

The National Institute of Standards and Technology (NIST) defined a *hash value (code)* as a "large number computed from the entire string of bits that form the file. The hash code (value) is computed in such a way that if one bit in the file is changed, a completely different hash code (value) is produced. To minimize the possibility that two different files may generate the same hash code (value), a sufficiently large hash value is computed."

Hash values can be used during discovery of electronic records to create a form of electronic "Bates stamp"[405] that will help establish the document as authentic. Grimm states in his judgment of *Lorraine v. Markel*[406] that:

> *"A* party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the final or legally operative version. This can plague a party seeking to introduce a favourable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. The use of hash values when creating the final or legally operative version of an electronic record can insert distinctive characteristics into it that allow its authentication."[407]

---

[404] Rothstein, Barbara Jacobs, Ronald J. Hedges, and Elizabeth Corinne Wiggins. *Managing discovery of electronic information: A pocket guide for judges* (Federal Judicial Centre, 2007), 24; see also Williams v. Sprint/United Mgmt. Comp., 230 F.R.D. 640, 655 (D. Kan. 2005).
[405] It means the process of applying set of identifying numbers to documents, for the purpose of identification.
[406] 241 F.R.D. 534 (D. Md. 2007)
[407] 241 F.R.D. 534 (D. Md. 2007) at 26.

3.4.5.5 Meta Data

Meta data is also a helpful tool to authenticate electronic evidence. It means "data about data" it is defined as, "information describing the history, tracking, or management of an electronic document.[408] Appendix F to The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age defines metadata as".

3.4.5.5.1. Cases

Mentioned below are two cases that suggest the effectiveness of using meta data as a tool for authenticating electronic evidence. One case, *Hagenbuch v. 3B6 Sistemi Electronic S.R.L,* [409] it was held that both parties must produce documents in its original form in which meta data can be produced. The issue arose when the defendant produced the document in TIFF (Tagged Image File Format) which does not contain metadata.

The observation made stated that, "It is clear that the TIFF documents do not contain all of the relevant, non-privileged information contained in the designated electronic media. The parties agree that, unlike the original electronic media, the TIFF documents do not contain information such as the creation and modification dates of a document, e-mail attachments and recipients, and metadata."[410]

The above two cases reveal the importance of a Meta data in authentication of electronic documents. The parties involved are under a duty to present the documents in their native format. However, we know that Meta data can be altered or tampered with.[411] There are though, methods for resolving such problems. Despite its lack of conclusiveness,

---

[408] Phillip J. Favro, A New Frontier In Electronic Discovery: Preserving And Obtaining Metadata, B.U. J. SCI. & TECH. L 13:1, 7.
[409] Hagenbuch v. 3B6 Sistemi Electronic Industrial S.R.L., No. 04 C 3109, 2006 WL 665005 (N.D. Ill. Mar. 8, 2006).
[410] Ibd. at *2.
[411] Lorraine v. Markel 241 F.R.D. 534 (D. Md. 2007) at 28.

however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

3.4.6 Communication Media Authentication

This section briefly discusses how the electronic evidence acquired from different online communication media are authenticated.

3.4.6.1. Web sites

Information appearing on private, government and corporate websites is usually proffered as evidence during trial. If the printouts of the web pages accurately show the content and pictures of the specific webpages, only then the webpages can be authenticated.

There are two types of websites; private and government. The government websites are usually self-authenticating. It only requires proof that the webpage does exist on the government website. For these types of websites, extrinsic evidence/oral testimony for authentication is usually not required. The reason for not requiring oral testimony is to avoid difficulty and inconvenience to the government officials. Also, generally with government sites, the risk of forgery or fraud is minimal. Websites of newspapers and journals are also exampling of self-authenticating websites. [412]

A website which contains a company logo and can be found at the URL address of the corporation is also authentic. It was held in the case *Denison v. Swaco Geolograph*

[412] Lorraine v. Markel American Ins. Co. 241 F.R.D. 534 (D. Md. 2007), at 18.

company[413] that, 'A business letter is authentic if it contains the logo or letterhead of the corporation through which the letter is originated'.[414]

For private websites the typical method of authentication website postings is through the testimony of "witness with knowledge". It was observed in the case *Illusions-Dallas Private Club, Inc. v. Steen*[415], that attorney presenting the affidavit for a party about obtaining a document from the website is not sufficient. This is based on the court observation, "there is no showing of personal knowledge that the studies are what they are claimed to be". Similarly, in the case *Wady v. Provident Life and Accident Insurance Co. of America*[416], it was commented that "holding that affiant cannot authenticate website postings, because he has "no personal knowledge of who maintains the website or authored the documents, or the accuracy of their contents... Courts disagree on how much knowledge is required".

A few courts have held that the proponent must offer the testimony from the owner of the website or webmaster. As in the case of, *United States v. Jackson*[417], it was held that, "proponent of information posted on white supremacist website must show that website sponsor posted the information, 'as opposed to being slipped onto the groups' websites by [the defendant] herself, who was a skilled computer user". In another case, Novak *v. Tucows, Inc.,*[418] it was observed by the court that, "Website printouts are not authenticated because the plaintiff offered no testimony or sworn statements by an employee of the companies hosting the sites".

---

[413] 941 F.2d 1416, 1423 (10 Cir. 1991).
[414] Steven Goode "The admissibility of electronic evidence." *Rev. Litig.* 29 (2009). 8.
[415] 2005 WL 1639211, at*10 (N. D. Tex. July 13, 2005), revised on other grounds, 482 F.3d 299 (5th Cir. 2007)
[416] 216 F. Supp. 2d 1060, 1064-65 (C. D. Cal. 2002)
[417] 208 F.3d 633, 637 (7 Cir. 2000).
[418] 2007 U.S. Dist. LEXIS 21269, at *5 (E.D.N.Y. March 26, 2007).

3.4.6.2 Social Network Messages

Many new types of writings, relevant as evidence in criminal and civil suits, are retrieved from the internet websites known as 'social networks'. Social networking websites allow their members to share information with others. Users create their own individual web pages (the profiles) on which they can post their personal photographs, information, videos, etc. And through their profile pages, they can send and receive messages. Anyone can create a profile on Facebook or Instagram free of cost. A detailed and well-written article on the issue is the one by Ira P. Robbins. [419]

The key issues in these social networks generated documents are typically one of the authorships i.e. the actual person who authored or posted the proffered document in question. Due to the increased risk of falsehoods and frauds with these types of mediums, courts have imposed a heavier burden of proof on social networks' messages and postings.

The lack of security in this medium leads to issues such as, possibility that a stranger has sent messages via other user accounts. Generally, there must be sufficient conforming circumstantial evidence to permit the inference that the purported sender was in fact the author. As for emails, the electronic signature on the documents must be corroborated with other proofs of identity of the author, such as application of the reply letter doctrine[420]. The Texas Rules of Evidence Handbook identifies a traditional method of authentication permitted by Rule 901 known as the "reply-letter doctrine". It means "a letter received in the due course of mail purportedly in answer to another letter is prima facie genuine and admissible without further proof of authenticity".[421]

---

[419] Ira P. Robbins, "Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence." *Minnesota journal of law, Science and Technology* 13. no1. (2013).
[420] Varkonyi v. State, 276 S. W. 3d 27, 35.
[421] Texas Rules of Evidence HandBook, Rule 901.

In general, there are three common methods of authentication of a social network profile or posting:

1. To ask the creator if he formed the profile and also if he added the postings in issue.
2. To search the computer of the person who allegedly created the profile and added the postings. It also includes an examination of the computer's internet history in hard drive to determine whether it was that specific computer which was used to originate the profile and postings in issue.
3. To obtain information directly from the social networking website that links the creation of the profile of the person who allegedly formed it and also links the postings with the person who initiated it.[422]

3.4.6.3 Instant Messages

One of the leading cases about chat room authentication is *United State v. Tank*[423]. It is a criminal case in which the defendant was accused of child pornography distribution. The defendant was a member of a chat room called *orchid club*, protected by password. The defendant used to discuss and trade images of pornography. Another member of the same club, Ronald Riva, was arrested on child molestation case. On search of Riva's house, police discovered that Riva had kept all the chats in his PC. The discussions in chat room implicated Tank. Those discussions were produced as evidence by the government. The defendant took a plea stating those discussions were not properly authentic. The court rejected the plea on the following two grounds:

---

[422] Robbins, "Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence", 28

[423] 200 F.3d 627 (9th Cir. 2000)

First, Riva testified as witness of the government. He told the court about how he created the logs. He further testified that the discussions saved on the computer were accurate record of the club discussions. Second, other circumstantial evidence led to the conclusion that the discussion was accurate. For instance, Tank admitted that the name he used during chat was "Cessna". A few other co-conspirators also testified that they used the name "Cessna" and "Cessna" appeared in the printouts on which chat room discussions were printed.

In another case, *Re. F.P.*, [424] the defendant, a minor, was accused of assault. The victim told the court that the defendant was angry because he thought the victim had stolen something from him. The court accepted instant message conversation between the victim and the defendant in which the defendant used the name "Icp4Life30". The defendant argued that he was not the author of these text messages and that those messages were not authentic. The court rejected the plea due to certain other circumstantial evidences involved in the case. For instance, during the first conversation the victim asked "Icp4Life30" who was he. The answer was the first name of the defendant. In addition to it, "Icp4Life30" many times accused the victim of stealing from him and talked about meeting with the school authorities.

3.4.6.4 Text Messages

Authenticity of text messages can also be established through circumstantial evidence. In the case of *In the interest of F.P.*, [425] the judge offered some robust and realistic comments on this topic which deserve to be repeated:

> "Essentially, appellant would have us create a whole new body of law just to deal with emails or instant messages. The argument is that email or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out,

[424] 878 A.2d 91, 95 (Sup. Ct. Pa. 2005)
[425] 878 A.2d 91, 95 (Sup. Ct. Pa. 2005)

anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationery can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework.... We see no justification for constructing unique rules for admissibility of electronic communications such as instant message; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundation showing of their relevance and authenticity." [426]

3.4.6.5 Emails

Emails are perhaps one of the most extensively used tools to transfer information in private, business and public sectors. They are admissible evidence. It is not a necessary requirement that along with email, details of the computer and its operating system must also be presented. In other words, means of authentication might not always require evidence from an expert.[427]

Admissibility of emails is often subjected to great misunderstanding.[428] There is a perception that emails can be easily forged[429], making it essential to provide evidence of authenticity. This perception is not correct. Documents typed on a paper can also be forged[430] and altered, as in the case of *Scholastic, Inc v Stouffer*[431], and letters can also be forged, as in the case of *Arrow Nominees, Inc v Blackledge* [432]. The forgery of a document is not a new phenomenon and just because there is a possibility that an email can be forged does not imply that email correspondence must be passed through an extensive forensic analysis to prove its authenticity for the purpose of admissibility. There are other equally effective ways of testing authenticity of an electronic document.

---

[426] Ibid. 95.
[427] ***DPP v Brian Meehan*** [2006] IECCA 104,
[428] Pennington s ***Beverly v Holset Engineering Limited, Bover v Schroder Securities Limited.***
[429] ***Munshani v Signal Lake Venture Fund II, LP,*** 805 N.E.2d 998, http://www.signallake.com/litigation
[430] Winsor C. Moore, 'The questioned typewritten document', Minnesota Law Review 43 (1959), pp 727-743.
[431] 221 F.Supp.2d 425 (S.D.N.Y. 2002), 2002 U.S. LEXIS 17531. See *Breezevale Limited v Dickinson,* 879 A.2d 957 (D.C. 2005), *Masood v Zahoor* [2008] EWHC 1034 (Ch); *Zahoor v Masood* [2009] EWCA Civ 650
[432] [2000] All ER (D) 854, [2000] 2 BCLC 167, [2001] BCC 591 reversing [1999] All ER (D) 1200, [2000] 1 BCLC 709.

Proving the authenticity of the email can also be done by use of metadata. The email header has metadata which indicates when an email is sent and received. The 'sent' time set in the sender's email-metadata would be the same as the 'received' time on the recipient's email-metadata. The metadata is auto-generated and cannot be changed. If the metadata shows a time, it means, the email was actually sent or received at that time. Secondly, in between the sender and receiver, there are several mail servers that connect to one another. The route traced by an email can also be traced. Therefore, metadata provides sufficient information to prove whether an email is forged or not. Such as, in the case of *Greene v. Associated Newspapers*[433], the email was analysed for the purpose of proving its authenticity. The emails were exchanged between Peter Foster and Martha Greene. Later on, Ms. Greene denied that she sent the emails to Mr. Foster and claimed that the emails were forged. An electronic evidence specialist who examined Greene's PC could not find any trace of the emails. However, a forensic expert inspected three emails on a laptop, owned by Mr. Foster at his house in Australia. The specialist was able to complete "Trace route" on the 'IP address headers' from the emails. This evidence was enough to show that the emails were sent from a server in a Greater London Area[434] which was the same as Ms Green's email-metadata. The mail servers traced from the email headers were also actual servers. And the times recorded by the email header also showed that the sending and receiving timings of the emails were accurate and coincided as well. As the email address header from the sender could not be altered, the mail could only have been sent from the sender's email. Although the sender of the email could have been another person who had access to the owner's PC. At the time of the inspection of email header, it showed that from the point of departure to the recipient's inbox, the emails had not been interfered with. The defendant's digital evidence expert stated that although the text of the email could be changed while forwarding or sending an email to

[433] *Greene v. Associated Newspapers* [2004] EWCA Civ. 1462, [2005] QB 972, [2005] 1 All ER 30.
[434] Ibid. 37.

oneself or to a third party, the original header would indicate such alteration. And in the given case there was no such indication in the header information of the emails. The Court of Appeal agreed with the trial judge that there was no clear evidence ('knock-out evidence') which showed that the email was a forgery[435].

Similar arguments were used in the case of *The People of the State of Illinois v. Downing*[436], where the expert witness testified that the only way of authentication of the origin of one of the emails in question was by investigating the IP address, which was not included in the exhibit as in the case *R v. Mawji (Rizwan)* where the relevant email contained admissions of guilt. [437]

3.5 Conclusion

In the light of the discussion presented in this chapter, the following conclusions can be drawn;

Criteria for admissibility are the same for both physical and electronic evidence. Evidence must be relevant for being admissible. Relevance becomes complicated when dealing with huge databases and servers. Recently, researchers are showing the involvement of electronic discovery motions[438] in majority trials are proving to be too expensive even for large multinational companies. So, the process of proving the relevance of an evidence must be reasonable and cost effective.

The second most important criteria for admissibility of electronic evidence is its authentication which is a complicated task. For that it is important to understand the type of a documents, i.e. computer generated or computer stored. The authentication of computer-

[435] *Greene v. Associated Newspaper Ltd.* [2004] EWCA Civ. 1462 at [21]
[436] 37 III. App. 3 d 297 (III. App. Ct. 1976)
[437] [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct).
[438] See chap 5, para 5.1.

generated data can be done by checking whether the system is working properly or not. But if the computer carries a statement fed by a human being it would fall under the category of hearsay. The issue of hearsay is important and hence been discussed in great detail in the following chapter.

Western law has introduced many types of authentication i.e, authentication by witness with knowledge, expert witness, authentication by circumstantial evidence, authentication through meta data, authentication by hash tags.

Authentication through witness with knowledge, expert witness and circumstantial evidence have already been discussed under Islamic law. [439] All the methods of authentication adopted worldwide are the same as have already been discussed 1400 years ago under the Islamic law.

[439] See Chap 2 above, para 2.3.3 to 2.3.6.

CHAPTER 4 ADMISSIBILITY OF ELECTRONIC EVIDENCE: THE SUBSEQUENT STAGE

4.1 Introduction

Modern western legal litigation involves electronic data in every form such as computer charts, timelines, digital recordings, websites data, instant messages, digital photographs, data call logs, metadata, etc. Lawyers invest a lot of time in requesting, assimilating, producing and generating a large amount of computer data. It has resulted in an enormous growth of electronic evidence in trials and court rooms.

Besides the issues related to authentication, a number of other issues exist with regards to electronic evidence which need to be dealt with. Two major issues include hearsay and best evidence rule. The traditional concepts of hearsay and original writing rule have considerably changed in electronic evidence. This chapter briefly discusses both the issues.

4.2 Hearsay Rule

4.2.1 Definition

Hearsay is the declaration made by someone other than the declarant, while testifying at court trial or hearing. This statement is offered as evidence to prove the truth of the matter asserted. Common law recognizes the rule against hearsay. It means hearsay evidence is inadmissible unless it falls under one of its exceptions. The perceived unreliability of hearsay evidence constitutes the main justification for recognizing a rule against hearsay.[440]

Hearsay evidence is not the best evidence and it is not delivered on oath. The truthfulness and accuracy of the person whose words are spoken to by another witness cannot be tested by cross-examination. The light which his demeanour would throw on his testimony

[440] Susan E.E.B. Sherman, "Hearsay and Evidence in the Computer Emergency Response Team (CERT)" SANS Institute Reading room site, (2005), 5. Also in Find Law, "Hearsay evidence", http://criminal.findlaw.com/criminal-procedure/hearsay-evidence.html (accessed January 4, 2017)

is lost.[441] Any statement may be unreliable because of defects in the perception, memory, sincerity, or ability to narrate clearly, of the maker of the statement.[442]

In his book, "Electronic Evidence: Law and Practice, Rice defines hearsay as;

> "Hearsay evidence can be defined as: an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination."[443]

Some hearsay exceptions are admissible in order to avoid problems. For example, if the testifying witness is incapable of coming to the court. Or a witness is a government official who cannot leave the office. Due to these reasons, exceptions are there that are admissible in court such as business records, public records, records of vital statistics, records of religious organizations certificates of baptism, marriage and related event and family records. [444]

4.2.2 Digital Evidence Issues and Rules

Hearsay issues are pervasive when electronically stored information is sought. There are issues such as, whether a statement made by a computer can be termed as hearsay or not. Law of evidence states that hearsay statements must be uttered by human beings. So, the issue

---

[441] Tepre v R [1952] AC 480-486.
[442]Margaret L Ross and James P Chalmers, "*Walker and Walker: mmmThe Law of Evidence in Scotland*" (West Sussex: Blooms berry, 2008), 123. (Accessed January 24, 2017) http://uk.practicallaw.com/books/9781845921651/chapter8
[443] Paul R. Rice, *Electronic Evidence: Law and Practice*, (Section of Litigation: American Bar Association, 2005), 262

[444] Law reform Commission of Ireland, Accessed January 24, 2017. http://www.lawreform.ie/_fileupload/consultation%20papers/wphearsay.htm

arises as to how a PC can be cross-examined, andr whether the PC "knows" something, and if it is an original thought or something that has been fed into it.[445]

Most of the communications nowadays are in electronic medium, such as, e-mails, text messages, chat rooms, internet postings, Facebook and YouTube. These electronic communications carry human statements. Communications include observations of events around, statements about plans, motives, and feelings. All of this data is transmitted through electronic medium.[446]

In the above-mentioned case when, a computer is serving to be a carrier of statement, the issue arises as to how to deal with it. For the purpose of establishing the evidential foundation of electronic data, the electronically stored information is broadly categorized into certain special categories. These terms are important in every evidence case. However, in the case of computer-based evidence, these terms become even more significant.

Based on type of electronic data, broadly, there are two kinds of electronic evidences;

1. Computer-generated evidence
2. Computer-stored evidence[447]

4.2.2.1 Computer-Generated Records

These records are generated from computer without human intervention. The definition of hearsay is not applicable in these records because, a "human" is not making any statement.

---

[445] Susan E.E.B. Sherman, Hearsay and Evidence in the Computer Emergency Response Team (CERT), 5.
[446] Lorraine v. Markel American Ins. Co. 241 F.R.D. 534 (D. Md. 2007)
[447] Nathan Judish, ed. *Searching and seizing computers and obtaining electronic evidence in criminal investigations* (Office of Legal Education, Executive Office for United States Attorneys, 2009). http://www.cybercrime.gov/s&smanual2002.htm. October 2004 (accessed: September 1, 2015). Also in Susan E.E.B, Hearsay and Evidence in the Computer Emergency Response Team (CERT), 5.

These statements are generated from computer. So, courts do not apply hearsay rules to computer generated records.[448]

Computer generated records are controlled by software program which do not carry input from a human. For instance, data logs, connections made by telephones, ATM transactions and evidence from a device fitted to the airbag system of the vehicles[449]. In these cases, items of software communicate to connect telephones (usually between two telephone numbers), and the software, written by a human, is instructed to record the telephone number being called and the number from which the call is being made for the purpose of charging for the call[450].

In *Lorraine v. Markel* [451] it was observed by court that: "An electronically generated record is entirely the product of the functioning of a computerized system or process, such as the report generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no person involved in the creation of the record, and no assertion being made. For that reason, the record is not a statement and cannot be hearsay."

A report by the Great Britain Law Commission was published in 1997. In paragraph 7.43 of that report[452] it was observed that "present laws draw a distinction according to whether the statement consists of, or is based upon, only what the machine itself has observed, or whether it incorporates or is based upon information supplied by a human being."

---

[448] A. Comment, A Reconsideration of the Admissibility of Computer-Generated Evidence, 126 U. PA. L. Rev. 425 (1977), Jerome J. Roberts, "A Practitioner's Primer on Computer-Generated Evidence." *The University of Chicago Law Review* 41. no. 2 (1974): 254-280.

[449] Antonio B. Singh was convicted of dangerous driving in Birmingham Crown Court and sentenced to 21 months' imprisonment in 2010.

[450] Rosemary Pattenden, "Authenticating "things" in English law: Principles for adducting tangible evidence in common law jury trials" *12 E & P*, (2008), 297.

[451] Lorraine v. Markel 241 F.R.D. 534 (D. Md. 2007)

[452] Great Britain and Law Commission, *Evidence in Criminal Proceedings: Hearsay and related topics* (HM Stationery Office, 1997), 100.

It was observed further that hearsay concept did not apply to photographs, films, or documents automatically recorded by a machine. It is rather real evidence and not hearsay.

Other cases are also there that exclude electronically generated records from hearsay. For instance, in the case *United States v. Rollins*, [453] it was observed that: "Computer generated records are not hearsay. The role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer-generated record in this case. Instead, the admissibility of the computer tracking system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy."[454]

Similarly, in the case *State v. Dunn,*[455] it was noted that "Because records of this type (computer generated telephone records) are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved."

Another case, *State v. Hall,*[456] observed that reviewing the admissibility of computer-generated records and holding "the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer-generated record in this case. Instead, the admissibility of the computer tracking system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy".

---

[453] 2004 WL 26780, at *9

[454] *State v. Hall* 976 S.W.2d 121, 147 (Tenn. 1998). Accessed January 24, 2017. https://casetext.com/case/state-v-hall-698.

[455] 7 S.W.3d 427, 432 (Mo. Ct. App. 2000)

[456] *State v. Hall* 976 S.W.2d 121, 147 (Tenn. 1998). Accessed January 24, 2017. https://casetext.com/case/state-v-hall-698.

In these cases, computer is performing calculations based on the programs. For example, a thermometer is used for checking the temperature of a human body. The figures taken from the thermometer are not statements. Automated tools or machines can never lie. So they are not hearsay. The tools may be reported to have errors or malfunctioning issues which can be fixed. Or in case of any tampering or alteration expert testimony can be adduced so that the gaps between the evidence can be filled. [457]

Smith discussed the types of representation, which can be made by computer.[458] He argued that computer can perform many functions by instructions, many of them are done through mechanical ways. For instance, time and date on an email. He said that in these cases, a computer is creating direct evidence and not hearsay.

Witness can be challenged about the truthfulness of their recollection of observation. Such evidence shall not be hearsay. On the other hand, accuracy of thermometer might be open for check up for that testimony of a qualified expert shall be adduced. [459]

The remaining examples quoted by Smith were of camera that record image, sound recorder or radar. In all these cases, if a witness lies about the reading from a computing device such as a radar, speedometer, etc., the evidence from such devices is not hearsay. Programme may make errors or mistake. He said that the "consideration goes to weight and not the admissibility" in these cases.

---

[457] Johanne Gauthier, "The Admissibility Of Computer-Generated Evidence: An Overview" Canadian Maritime Law Associates, November, 5. .

[458] J.C Smith, "The admissibility of statements by computer" *Criminal Law Review* (JUN 1981), 387.

[459] Penelope A. Pengilley, "Machine information: Is it hearsay?" *Melbourne University Law Review 13* (1982), 625.

4.2.2.1.1 Admissibility Criteria

Three aspects must be considered while analysing the computer-generated evidence for admissibility are that the computer has capability to process only the information that is fed into it. If there is a mistake in information which is undetected, the error shall be undetected. And if the computer is asked to process the data which is incomplete or inaccurate, the results too shall have the error. If there is a deficiency in the manner in which a computer is told to process the data, the results too shall have problems.[460]

Other important factors for admissibility of computer-generated records are that the computer-generated record should have been prepared in the ordinary course of business. And the business must be heavily relying on the data i.e. the data is completely trusted upon for running the business.

The chain of custody and the way the data is preserved is the most essential characteristic of reliable business record. For instance, in the case of *D and H Auto parts v. Ford marketing corp.*[461], Ford offered to show the amount of sales from Ford part distribution with the support of documents. He presented the printouts. Defence challenged the accuracy of these documents. It was held that these printouts are admissible as they were being used for the business's own exhibits. Another court stated that the printouts prepared in the ordinary course of business has an aura of reliability. The creation of business record is deemed important but their safe and secure preservation is of utmost importance which was held in the case.[462]

---

[460] Jerome J. Robert, "A practitioner's primer on computer-generated evidence", *The university of Chicago. Law Review* 41, no. 2, 256.

[461] 57 FRD 548 (E.D.N. Y 1973)

[462] Robert " A practitioners primer on computer generated evidence", 258.

4.2.2.2 Computer-Stored Records

This type of information is usually based on manually intervened communication that is stored electronically. "Emails, word processing files, and even the columns that people enter into spreadsheets have human intervention. If the person who entered the information does not testify about it (and also be cross-examined in person and under oath on it), it is hearsay. If an attorney wants to enter an email into evidence, a proper exception/exclusion to the hearsay rule would be required". [463]

Some electronic evidence is hearsay, like, a printed piece of paper on which facts of an event are mentioned other than metadata. Such evidence is not admissible without proof. There are other pieces of evidence which contain both hearsay and non hearsay evidence. For instance, an email comprising facts of an event and header information. In these cases, proponent has to prove both kinds of evidence. [464]

The evidential foundation in the cases of this electronic evidence category where human and machine input is partially involved, are subjected to the accuracy and integrity of systems that were involved in processing. The human statements involved in the record would be hearsay and will be subjected to the testimony. It would require the oral testimony of a person who entered the data. If that person is not available, anyone who was the custodian of the record can testify. He must ensure the court that the statement entered is in due course of business and that the record is free from falsification or alteration.

---

[463] Susan E.E.B. Sherman, Esq. *"Hearsay and Evidence in the Computer Emergency Response Team (CERT)"* http://www.sans.org/reading-room/whitepapers/legal/hearsay-evidence-computer-emergency-response-team-cert-1541

[464] Mason, *Electronic Evidence*, 109

4.2.3 Exceptions

4.2.3.1 Business Records

Many jurisdictions include statutory exceptions to the rule against hearsay. One of those exceptions is to allow business records to be admitted as part of the organization's records. The documents can be included by a single person, organization or a body in the course of or for the purpose of business. Authentication of such records is maintained by the way of their entry in the records. Judges also ensure safe custody of these records. If they are formed in the ordinary course of business, they are admissible, considered as authentic and are subjected to the approval of the method of entry and custody of records. [465]

A copy of a business record is produced in the court on a presumption that the copy is an accurate reproduction of the original record. Due to this rule, the party tendering the copies will not be required to call the evidence to prove the accuracy of the device that has produced the evidence. Nor will they be required to prove the process that has produced the record as correct, unless the opposing party opposes it by adducing evidence to rebut the presumption. [466]

For admissibility, it must be proved that the business records were entered in the ordinary books of the bank and entry was made in an ordinary course of business. Other facts to be proved would be that the bank book was in the custody or control of the bank. [467]

The reason for the presumption of accuracy of business record is that business relies on certain records in day to day transaction which develop a certain level of trustworthiness. [468]

---

[465] *Lorraine v. Markel*, 241 F.R.D. 534 (D. Md. 2007)
[466] Mason, *Electronic Evidence*, 256.
[467] Qanoon-e-Shadat Order, article 48.
[468] R v Lemay (2004) 227 W
AC 279.

Secondly, as a normal course of a business, the employees are under an obligation to record, observe and report the facts correctly.

Generally, the court will accept the authenticity of electronic data, where evidence is proffered that the system which has produced the data is used on a regular basis. And the system is relied upon in the normal course of business.[469]

4.2.3.2 Public Records

Public records, similar to business records, do not require authentication by oral testimony. These documents have a presumption of truth attached to them. The validity of such documents will not be checked unless the other party challenge their validity. There are number of relevant cases on this subject. For instance, *United States v. Smith.*[470] when the court considered that computer printouts, submitted by the police, are admissible evidence because it is public document. Similarly, in *Hughes v. United States*[471], it was held that computerized IRS[472] printouts are admissible.

Public records include, Domestic public documents with and without seal and a document purporting to bear the signature in the official capacity of an officer or employee of any entity. Foreign public documents are also called public documents i.e a document purporting to be executed or attested in an official capacity by a person authorized by the laws of a foreign country to make the execution or attestation. Official publications, books, pamphlets, or other publications purporting to be issued by public authority are also public documents. Newspapers and periodicals are also public documents.

---

[469] Eleanor Swift, "Abolishing the Hearsay Rule", *Cal. L. Rev* 75 no. 495 (1987), 514. http://scholarship.law.berkeley.edu/californialawreview/vol75/iss1/21 (accessed May 10, 2017)

[470] 973 F.2d 603, 605 (8th Cir. 1992)

[471] 953 F.2d 531, 540 (9th Cir. 1992)

[472] The Internal Revenue Service (IRS) is a U.S. government agency responsible for the collection of taxes and enforcement of tax laws.

4.3 Best Evidence Rule

Best Evidence Rule is the fourth and last stage of admissibility. It is also one of the basic requirements that the evidence rendered in the court, must be original, real, primary, and direct. The doctrine of best evidence rule is based on the same notion that a high level of trust and integrity must be established when the best evidence is presented before the court.

Best evidence rule was earlier known as original writing rule wherein the proponent has to prove the content of writing, recording or photograph, as original. The duplicate will be admissible if the proponent can prove that the original is lost or destroyed. The original will also not be required if it is not obtainable by court. [473]

This principle applies to documents, photographs and recordings. If there is content in the document which requires of testimony, the party offering the testimony must provide the original of the writing, document, or recording. This rule is applied far less strictly under the electronic data in contrast to the physical evidence. [474]

The traditional principle of documentary evidence "Best Evidence", interpreted as a requirement of the original copy, is an impractical requirement with regards to electron records. Researches have shown that Best evidence rule is meaningless in the electronic environment.[475]

The reason of this view is the absence of an original record in the digital environment. But it is necessary to refer to an unbroken line of traces left by all those who interacted

[473] Rule X of Federal Rule of Evidence of USA.
[474] USA's Federal Rules of Evidence, Rule no. 1002
[475] Luciana Duranti, Corinne Rogers, "Trust in digital records: An increasingly cloudy legal area", *Computer Law and Security Law Review* 28, (2012), 527.

with the record or to the legitimate custody of a professional who can account for them.[476] It is possible to prove about the electronic records that they have the "force of original".[477]

The copies produced through a mechanical process are exactly identical to the original. There may be little difference in the hidden information (Meta data) but the main text is the same. If the record is kept in the safe custody and produced in the ordinary course of business, there is no problem in admitting copies. The copies, no doubt would be subject to provenance.

There are many countries in world that have legalized secondary evidence by force of law. However, there are some states in USA, [478] that still have the Original writing rule in place. But these states, by virtue of practice, are no longer capable of keeping up with the original writing rule. They have not explicitly legislated or stated that they have abolished the original writing rule but their course of practice and decisions depict that they have curtailed the use of this principle in the case of electronically stored information.

Paul Rice in his book, Electronic Evidence theory and Practice, states that:

> "For practical purposes, best evidence objections have been eliminated in federal courts (of America) as well, because mechanically produced copies of documents, denoted "duplicates," are as admissible as originals unless a genuine question of accuracy is raised by the opponent. Because virtually everything produced in electronic world is produced mechanically, once a document has been properly authenticated, the best evidence or original writing rule should pose no problems."[479]

---

[476] Luciana Duranti, Corinne Rogers, And Anthony Sheppard, "Electronic Records and the law of evidence in Canada: the uniform electronic evidence act twelve years later", *Archivaria*70, (2010)
[477] Paul Rice, *Electronic Evidence: Law and Practice*, 191.
[478] USA's Federal Rules of evidence clearly stipulated in Rule 10 that the evidence presented in the court should be "Best Evidence". (Accessed January 24, 2017) https://www.law.cornell.edu/rules/frc
[479] Paul Rice, *Electronic Evidence*, 190

4.3.1 Legislations Abolishing the Original Writing Rule

Best evidence rule was brought into force in order to minimize the risk of admitting unreliable and inaccurate records resulting from hand copying. However, all the digital duplicates are identical (though the Meta data may be different). The reason is that the source from which they are generated is single. So, the reliability of the computer comes out not from the record but from the integrity of the system. The system which generates, stores such documents. [480]

For instance, in Canada, it was legislated in Canadian Evidence Act (s. 31) that;

> "1. Authentication is of the computer system, not the record
>
> 2. The best evidence rule is satisfied by evidence showing the integrity of system"[481]

The above-mentioned electronic record provisions maintain that the best evidence rule is satisfied by the integrity of the system rather than relying on the originality of the record because the system is controlling the document. The best evidence rule is applicable in hand written documents. Keeping in view the above-mentioned facts, the best evidence rule seems to be inapplicable in the digital environment.

There are some states of Australia, which totally abolished the Original Writing Rule. Today the Evidence Act of the Commonwealth, New South Wales, Tasmania and the Acts are identical.[482] In each of these jurisdictions the best evidence rule has been abolished. Section 51 of each of the Acts entitled 'Original Document Rule Abolished', provides: "The

---

[480] Gauthier, "*The Admissibility Of Computer-Generated Evidence: An Overview*" 8.
[481] Canadian Evidence Act (s. 31)
[482] *Evidence Act 1995* (Cth); *Evidence Act 1995* (NSW); *Evidence Act 2001* (Tas). *The ACT applies the Commonwealth Act.*

principles and rules of the common law that relate to the mean of proving the content of the document are abolished".[483]

4.3.2 Hard Copies of Electronic Records as Evidence

When the original document is in electronic form, an issue may arise regarding whether the hard copy such as a printout is admissible into the court of law or not. For instance, some organizations print out the hard copy of emails and keep them as a 'permanent record' and delete the electronic version. These organizations are faced with the ruling which considers printout as inadmissible, thus jeopardize their opportunity to submit relevant evidence before the court. Law affirms that adopting this practice is professionally a negligent behaviour. The printout is inferior to the digital documents. [484]

This practice in an unnecessary hangover inherited from the early days of computers being used for commercial objectives in the 1970's and 1980's when computer space was expensive and computer specialists advised and required the users to 'clean out' the computer space for best efficiency. In this century, computer space is plentiful and cheap. There are many professional methods of archiving and saving such documents, records and communications.

In the US case, *Armstrong v. Executive of the President*[485], the court held that the Federal Records Act requires certain executive branch agencies to archive the electronic version of its e-mails. The defendants unsuccessfully argued that e-mail print-outs were the logical equivalent of electronic material, and consequently there should be no

---

[483] Alan Davidson, *The Law of Electronic Commerce*, (New Delhi: Cambridge University Press, 2009), 309.
[484] Ibid.
[485] Armstrong v. Executive Office of the President, 1 F. 3d 1270 (D.C. Cir. 1993).

obligation to archive superfluous electronic "copies."[486] In rejecting that argument, the court found that printed computer records, particularly printed email, do not display all of the information contained in electronic documents. Without specifically mentioning the term "metadata", the court detailed some of the embedded information found in e-mail that often cannot be viewed in hard copy; "important information present in the e-mail system, such as who sent a document, who received it, and when that person received it, will not always appear on the computer screen and so will not be preserved on the paper print-out."

By failing to include electronic materials in its archived records, the defendants' files comprised of an incomplete record, replete with what the court characterized as "dismembered documents" and "amputated paper print-outs." The Armstrong decision is noteworthy for several reasons. While there were other decisions that previously acknowledged the primacy of digital material over hard copies, the Armstrong court was perhaps the first to recognize the role of metadata in establishing that pecking order.[487]When the question of such a document arises it is clear that the jurisdictions where this rule is abolished, greater weight will be given to the electronic document. It would be of concern to the court that why the original was destroyed, especially when it contained the information which would have assisted the court in sustaining the document's originality and accuracy.

---

[486]Id 1285.

[487] Favro. Phillip J. "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata". *B.U. J. SCI. & TECH. L* 13. no. 1 (2007): 15. Accessed. May 9. 2017. https://ssrn.com/abstract=2255160

4.4 Conclusion

Electronic evidence must not be hearsay. For ascertaining the level of hearsay in electronic evidence, the categorization of computer generated and computer stored evidence must be considered. Generally, computer generated evidence does not carry hearsay. Computer stored evidence carries hearsay and needs oral testimony on the information stored on computer.

If an electronic evidence has component of hearsay in it, they must fall within the exception of the hearsay rule. The most important of them are business records, public documents and bankers' books. Business records cannot be blindly trusted as it is very important to see whether they were generated in ordinary course of business and that the method of preservation of such records is completely secure.

The concept of best evidence rule has entirely changed in the realm of electronic evidence. Earlier the law stated that only the original copy of the document, duly attested by witness, shall be admissible in court. But in the electronic field, a document generated by a computer is original irrespective of how many they might be, subject to the condition that the system which generated the document is a reliable and fool proof system. All the generated copies will be primary evidence and will be considered as original.

As a general principle, countries where Best Evidence rule is applicable, courts must dictate that the printout is not admissible. There are a number of exceptions to this rule. For

instance, destroyed or lost documents and public documents. However, courts should not accept copies where the documents were deliberately destroyed. [488]

In jurisdictions where the best evidence rule has been abolished, greater weight should be given to the digital document. Destroying the original copy in preference to the printed hard copy, risks the admissibility of unreliable documents or being given less weight. The court should question as to why the 'original' electronic documents have been destroyed, as they carry the information which assists court in substantiating the accuracy or originality.

Globally the states, have accepted that no evidence should be rejected on the ground that it is derived from the modern means of proof. It has been unanimously agreed that electronic evidence should not be treated as a "fruit of a poisoned tree". [489]Because most of the matters in society are regulated through electronic data. It administers Commercial, non-profit organizations, public, private organizations, and academia.

As previously stated, the basic structure of law of evidence is the same for trying electronic evidence in court, like the stages of admissibility and means of proofs etc. But once electronic evidence is involved in the case a number of differences add in a trial. Things from the physical world move to the virtual world in cyber cases. Today, technology is advancing at a lightning speed. Lack of technical knowledge and day to day advancement in the field of information technology is making this field more complex.

---

[488] See RA Brown, Documentary evidence in Australia, 2nd Edn. LBC Information Services, Sydney, 1996, 128-29.

[489] This doctrine establishes the illicit character of evidence obtained by a procedure that is shown to be marred, making them contaminated by the illegality of the procedure. Fredesvinda insa et.all., The admissibility of electronic evidence in court: fighting against high-tech crime Journal Of Digital Forensic Practice Vol. 1 , Iss. 4,2007 . It is also defined by Nolo Dictionary that "in criminal law, the doctrine that evidence discovered through unconstitutional means (such as forced confession or illegal search and seizure), may not be used as evidence against a criminal defendant.

The procedural laws have also been changed much by the advent of electronic evidence by many states.[490] After completion of the four-step analysis for the admissibility of electronic evidence, in the last two chapters, it is imperative to check the practical implication of e-evidence in civil and criminal cases.

There has been enormous growth in the volume of digital evidence both in civil and criminal trials. The use of electronic evidence is different both in civil and criminal trials. For instance, the process of investigation, in criminal cases the objects and premises are seized by the investigating officer and cannot be possessed by the parties. While in civil trials, parties stay in the possession of the data or the material. And parties are under bound to disclose the information to each other. [491]

[490] Like USA see Federal Rules of Civil Procedure.

[491] Larry Daniel and Lars Daniel, *Digital Forensics for legal professionals: Understanding digital evidence from warrant to court room* (Waltham: Elsvier, 2012), 113

CHAPTER 5 ELECTRONIC EVIDENCE IN CIVIL AND CRIMINAL TRIALS

5.1 Civil Trials: Electronic Discovery

In a civil case, each party makes a list of the documents and submits application in the court to get access to so and so documents. This is called the process of discovery. The civil procedural rules govern the problems related to trial, from initialization of proceedings to appeals. While electronic evidence problems may be created in many stages, they were most hard at the time at the of "document discovery"[492]. Electronic evidence is particularly hard to be located during the discovery stage, called electronic discovery (e-discovery). Today e-discovery has become the most challenging task for the investigation officers and lawyers.

5.1.1 Definition

Electronic discovery can be defined as, "any process (or series of processes) in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case". Evidence by the order of court or government sanctioned inspection for obtaining critical evidence is also a type of E-Discovery. It can be carried out offline or it can take place across a network. [493] The plaintiff should be in a position to show the actual type of electronic evidence required, the location and the person in control of the evidence.

The chances of destruction of evidence are higher in civil cases than in criminal cases. Because the person in control of evidence in civil cases may know that he will be asked to disclose the evidence to the other party. So, he may dispose of anything which is

---

[492] For details about e-discovery see, Michael R. Arkfeld, *Electronic discovery and evidence* (Law Partner Pub., 2005).

[493] Jack G. Conrad, E-Discovery Revisited: The Need for Artificial Intelligence Beyond Information Retrieval Artif Intell Law (2010) 18:321–345 DOI 10.1007/s10506-010-9096-6
(Accessed January 30, 2017) https://www.researchgate.net/publication/220539249_E-Discovery_revisited_The_need_for_artificial_intelligence_beyond_information_retrieval

incriminating him. On the other hand, in criminal cases the evidence is typically seized without any forewarning, thus lowering the chances of destruction of evidence. [494]

In discovery cases, parties exchange documents that are substantial to the fair adjudication of their dispute. It prevents the unconscionable concealment of information. Discovery should not be misused by the parties on a 'fishing expedition', in order to add litigation cost to the opposing party or to use it as a delaying tactic[495]. This is a unilateral obligation with which each party must comply, and is typically completed at the end of the pleadings. Documentary discovery is generally composed of two steps. Firstly, the party makes a list of all relevant documents which it has in possession[496], and provides this list to other parties as well as submits it to the court. Secondly, the opposition parties are formally entitled to investigate and obtain copies of the relevant and non-privileged documents.[497]

The major works done on electronic discovery include, Sedona Conference guidelines on electronic document production[498]. American Bar Association's Civil Discovery Standards, have also contributed much on the subject. It incorporates the recommendations of the Electronic Discovery Task Force of the ABA's Section of Litigation.[499] Sedona guidelines are incorporated by many Countries. Many countries have issued their own Electronic Discovery Guidelines[500]. Though the guidelines are not binding, but they 'give a proper framework to

---

[494] Larry Daniel and Lars Daniel, *"Digital Forensics for legal professionals: Understanding digital evidence from warrant to court room"* (Waltham: Elsevier, 2012), 113.

[495] Ter Kah Leng, E-Discovery of electronically stored information in commercial litigation, Computer law and security Review 30 (2014), 171.

[496] In some jurisdictions the list is just a list, but most typically the 'list' takes the form of an affidavit or sworn statement by the party to the effect that the list contains all known relevant documents (e.g Nova Scotia Rule 15, Ontario Rule 30.03). The latter type of rule often imposes the additional requirement that council swear that he/she has explained the discovery obligation to his or her client.

[497] For instance, Nova Scotia Rule 14, Ontario Rule 30.10

[498] The Sedona Conference, The Sedona Principles Addressing Electronic Document Production, Second Edition, Sedona, AZ, June, 2007. As of September 19, 2007: http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ ed_607.pdf

[499] American Bar Association's Civil Discovery Standards, Chicago, IL, August 2004. As f September 19, 2007: http:// www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf

[500] Guidelines for The Discovery of Electronic Documents In Ontario. Acessed: January 30, 2017) http://www.oba.org/en/pdf_newsletter/E-DiscoveryGuidelines.pdf.

address how to conduct e-discovery, based on norms which the legal practitioners can adapt and grow with the passage of time as a matter of practice.'[501] USA and many other countries have amended their civil procedure codes keeping in view the problems posed by electronic discovery.[502]

5.1.2 Legal and Economic Issues

Dealing with electronic data is a helpful tool in all fields of life if it is utilized and managed properly. Or else, it can pose serious issues such as unmanaged volumes and complexity of electronic data, increased cost of trial, problems for the legal practitioners and their clients, which in turn can cause businesses to face increased operational costs while handling e-discovery cases.[503] Generally, the rules that are applicable to discovery of physical discovery are applied to electronic data as well. Electronic discovery can influence the outcomes and cost of the cases as well. It has been observed in a large number of cases that electronic discovery motions have posed serious cost issues such as production costs, increase in data or volume shall increase the scale of review of attorney which will eventually increase the attorney fees. Electronic discovery can also pose some other challenges such as severe sanctions or loss of attorney-client privilege.[504] The use of efficient and low-price mediums for storage of electronic data can somewhat reduce the cost of discovery cases.

If any kind of information is provided which can change the perception of trial, or strengthen the case of plaintiff, then demands for settlement shall increase.

---

[501] Ontario Bar Association, *Guidelines*, pp 1 – 2. Prior to the release of *The Sedona Canada Principles* (regarding which see below), the OBA Guidelines were beginning to appear with some frequency in the case reports; see *Sycor Technology Inc. v Kiaer*, 2005 CanLII 46736 (Ont. SCJ); *Air Canada v WestJet Airlines Ltd.*, 2006 CanLII 14966 (Ont. SCJ); *Spielo Manufacturing Inc. v Doucet*, 2007 NBCA 85; *Andersen v St. Jude Medical Inc.*, [2008] O.J. No. 430 (Ont. SCJ).

[502] See Rule 34 of Federal Rules of Civil Procedure of USA.

[503] James Dertouzos, Nicolas M. Pace and Robert H. Anderson, *The Legal and Economic Implications of Electronic Discovery* (Santa Monica: Rand Corporations, 2008), 10.

[504] Ibid, 12.

Karl Von Clausewitz discussed about 19th Century War and said, "Everything in (war) is very simple. But the simplest thing is very difficult." However, his statement is easily applicable to electronic discovery in the 21st century. Back in the past (mid-1990s), the concept of electronic discovery was confined to the examination of hard drives, floppy disks and CD-ROMS etc. The modern Internet Age ushered in online investigations, Web site defacement, e-mail and the tracking of hackers. Today everything and everyone is online and wireless. Each investigation carries a digital component, and most of the people are doing digital forensics in one way or the other.[505]

A court can demand parties at litigation to discover all relevant documents which are in their possession, custody or control. The term 'documents' has been interpreted generally and widely by the courts to include electronic files, databases and the physical media on which they are stored. For instance, hard drives, DVDs, USB sticks, SD cards and back-up tapes, etc.[506] In practice, it is necessary for the parties to be careful when listing 'document' in any discovery, as highlighted in the case of *GT Corporation v. Amare*[507], where one party had discovered a number of forensic images, which later ascertained that these images contained privileged material.[508]

---

[505]Ibid. 145

[506]*Sony Music Entertainment Ltd (Australia) v University of Tasmania* [2003 FCA 532.

[507] GT *Corporation Pty Ltd v. Amare Safety Pty Ltd* [2007] VSC 123.

[508]The legal dictionary by Farlex define privileged communication as confidential communication. Due to public policy there are some relationships which are considered to be confidential and they are privileged to be disclosed by
awitness. A witness cannot refuse to testify about a matter disclosed in a private conversation inconfidence and i n reliance upon the witness's promise of secrecy unless the law recognizes it as a confidential communication. Certain communications arising between an attorney and client, a Husband and Wife, priest and penintent and a physician and patient are privileged against disclosure by a witness. https://legal-dictionary.thefreedictionary.com/communication (Acessed April 14, 2018)

Majority of the common law countries have revised their rules of discovery because the previous rules of physical document discovery are not very effective.[509] Therefore, the rules governing discovery can sometimes produce anomalies in the context of electronically stored information. Electronic information is practically impossible to eliminate entirely. The parties may be unaware of electronic documents that are in their possession, custody or control. For example, emails that have been deleted may still be investigated from the hard drive or servers. For the sake of complete discovery, a digital evidence specialist may have to be engaged to extract information in the form of digital footprints.[510]

5.1.4 Case Study; UBS vs. Zubulake, [511]

In this case person called UBS hired Miss Zubulake, (Laura), as a director sale, in August 1999. Initially Laura was working under Dominic Vail. She was told at the time of hiring that she will be considered for the job if Dominic left, but this did not happen and UBS hired Chapin.

Laura filed a suit of gender discrimination with the Equal Employment Opportunity Commission on August 16, 2001. She stated that she was the only female on the desk and the defendant harassed her sexually and insulted her number of times in front of the co-workers. She was terminated from the job on October 9, 2001. The nature of the case demanded the electronic discovery procedure of emails of both the employees, Laura and UBS. Discovery commenced around June 3, 2002. Laura's first discovery request included, "All documents concerning any communication by or between UBS employees concerning Plaintiff."

As a result, UBS presented three hundred and fifty pages in documents in response of Laura's request, in which almost hundred pages of email messages. After presentation, debate

---

[509] Ter Kah Leng, E-Discovery of electronically stored information, 172
[510] *R v Spibly* (1990) 91 Cr App Rep 186, [1991] Crim LR 199 at 202, CA.
[511] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

increased and Lura demanded discovery of more emails. UBS did not give any other emails and said that further discovery demands are too costly.

It was noted that Laura produced 450 pages and on the side of UBS from those conversations had been deleted. Court ordered UBS to show how his system of back up protocols worked? Court observed "1. Because of the way back up system of UBS was designed, UBS could search all its archived emails without restoring all the backup tapes, and (2) There are more pages of responsive emails produced by Laura (450) than the totality of UBS (100) leading the court to conclude there were more emails to discover".

This was the case when it was realized by the courts that Electronic discovery is costing very high, which is burdensome on the defendant parties. Because, previously it was a rule that defendant party shall bare the expenses of discovery. The court then proceeded to conduct a cost analysis while contemplating whether Laura and UBS should share the costs of the backup restoration. It was the first time when courts decided that both the parties should share the cost in order to mitigate the loss. The court ordered the share of the cost by the ratio of 75 and 25 percent.

It was proved that some emails were deleted despite UBS instruction to the contrary. Court decided to put sactions on UBS for not being able to preserve certain data. It was found out that number of backup tapes were missing and "isolated e-mails created after UBS supposedly began retaining all relevant e-mails were deleted from UBS." Zubulake also started a motion of spoliation against UBS.

After the evidence and witness, the court was able to conclude that UBS acted wilfully and granted the adverse inference against them.

> "You have heard that UBS failed to produce some of the e-mails sent or received by UBS personnel in August and September 2001. Plaintiff has argued that this evidence was in defendants' control and would have proven facts material to the

matter in controversy. If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavourable to UBS".[512]

The jury ultimately decided for Zubulake awarding "$9.1 million in compensatory damages, and $20.2 million in punitive damages"

The above-mentioned case was a breakthrough in history of electronic discovery. It was deterring for the other business enterprises. In the above-mentioned case, a number of issues were confronted and addressed. The first one was of cost of electronic discovery. Electronic discovery is charging too high which is burdensome for defendant. In this case, the cost was shared among the plaintiff and defendant both. The second is the data retention policies of companies. Deletion of data can be suicidal for business tycoons. It can compromise their reputation. That is the reason why the attention of law researchers was attracted towards this issue. Needs of suitable policies were already felt, which were further strengthened by this case.

5.1.5 Cloud Computing; Proposed Solution

The National Institute of Standards and Technology defines cloud computing as;

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or services provider interactions". [513]

The services that are available in cloud computing generally require a reasonable periodic service fee and some more hardware cost, which is generally little, to access the

[512] at 439-40d

[513] Peter Mell and Tim Grance. "The NIST definition of cloud computing." (2011).

computing solutions. In cloud computing the Cost of IT assets, which is generally too high, is quite low. Removal of software license charges and software maintenance cost, together makes a very economic model. The user enjoys turnkey solutions supported and maintained by the service providers, and hosted at a remote location. Cloud computing is enabled by rapid, reliable internet and mobile data communication, which means that applications and data are available "everywhere" simultaneously and transparently. The convenience and financial benefits of cloud solutions are changing business models fundamentally and have resulted in mass migration of data to the cloud. [514]

The cost of storage in cloud computing is relatively very low and it can create entirely new storage areas.[515] Cloud computing is utilized as an effective tool for conducting sound forensic investigations. It helps in preserving remote images of virtual images. In this case the investigator has to trust to preserve and then to retrieve the evidence in forensically sound method. [516]

5.1.6 Other Solutions

Lawyers are using the results of an e-Discovery process and they initially order production of certain documents and their examination. It is important that the procedures are well organized to enhance the effectiveness of the court case.[517]

Storage of data is becoming more economical and easier. There are a few organizations that have electronic document retention and deletion policies. And fewer have litigation hold

[514] James P. Martin and Harry Cendrowski, *Cloud computing and Electronic Discovery*, 33.
[515] Ibid
[516] Stephen O' Shaughnessy and Anthony Keane, Impact of Cloud Computing on Digital Forensic Investigations. In *IFIP International Conference on Digital Forensics*, pp. 291-303. Springer, Berlin, Heidelberg, 2013.
[517] Dario Forte, Richard Power, Electronic discovery: digital forensics and beyond, 9.

policies to stop document deletion when litigation is expected to be commenced or has already commenced. The increased use of electronic communications and paperless records have posed many hurdles for businesses to monitor record retention policies. These deficiencies can pose serious threats for companies if they fail to comply with the record retention requirements and get indulged in litigation. If their policies are not according to the legal standards, these companies can face serious civil and criminal sanctions and costly recovery efforts. [518]

Despite the repeated argument that with the arrival of electronic discovery, burden of searching voluminous data has increased on the defendant, electronic discovery can be more of a help for reducing the burden. Many have argued that searching in electronic discovery can be cost prohibitive which might not result in any useful output. Proportionality principle was an effort for solving this problem.[519]

Supreme Court of USA argued in 1978 that the purpose of using electronic information is to reduce the costs.[520] Word searches, in case of electronic data, is much easier than manually searching the same word in hard copy of data. Some reports have realized that savings have not been realized and burdens have multiplied. The discovery can be much more convenient and less costly if it is undertaken by electronic means other than page-by-page review.[521]

Some modern developments suggest that searching and locating e-mail is not that difficult. It was also reported that plaintiff's attorneys used a computer programme to locate the emails which were required by them. Employers also download "electronic sniffers" to identify email communications which are contradictory to their email policies. Some of them

---

[518] Ibid. 10.
[519] Richard L. Marcus, Confronting the Future: Coping with Discovery of Electronic Material, *Law and Contemporary Problems*, vol. 64, No 2/3 (Spring-Summer 2001), PP.260.
[520] Oppenheimer Fund, Inc. V Sanders, 437 U.S. 340, 362 (1978). Also, in Richard L. Marcus, Confronting the Future: Coping with Discovery of Electronic Material, 260.
[521] Richard L. Marcus, Confronting the Future: Coping with Discovery of Electronic Material, 262

have started installing additional hard disks which are saving every keystroke to monitor the activities of their employees.[522]

5.1.7 Procedure of Electronic Discovery

The procedure of electronic discovery entails mapping, collecting, elaborating, and presenting documents in a legal case or an audit. It is a very complex process for two main reasons;

1) The electronic data will come from a variety of sources; for instance, emails, log files, transactions scanned files (Optical Character Recognition - OCR) and office documents, etc., and therefore be very heterogeneous.

2.) Apart from the trustworthiness of individual files, there is also the practical problem of file redundancy. Especially in teamwork contexts, there will be various versions of any given file or document, and it may be difficult or impossible to find the most recent one.[523]

5.1.7.1 The Prerequisites

In their book titled "Digital Forensics for Legal Professionals: Understanding Digital Evidence from Warrant to Court Room", the authors describe that there are certain prerequisites for the electronic discovery. These pre-requisites are important for starting a motion in the court.

1. Importance of Timings: Timing is the most important element for electronic evidence. It is not necessary that electronic evidence is lost due to delay in creation and collection. But there are many examples when computer windows crash, companies delete data in normal

[522] Ibid.

[523] Dario Forte (CFE, CISM), Richard Power, "Electronic discovery: digital forensics and beyond", Computer Fraud security Volume 2006, Issue 4, April 2006, Pages 8–10. Accessed January 26, 2017. http://www.sciencedirect.com/science/article/pii/S1361372306703323

business routine, cell phones are discarded. Big companies upgrade their system and delete the previous data. Thus, the nature of electronic evidence is volatile.[524]

2. Locating the Evidence: In civil case discovery, the main purpose of the "investigation" is to locate and collect electronic evidence. The same steps of this investigative process may be used in a criminal investigation. It involves answer to the following questions;

i) What is the Source of Electronic Evidence? There are many methods through which electronic data comes into existence. For instance, everything from phones to automated parking systems can create an electronic record. ATM machines with cameras, mobile phones, surveillance systems, alarm systems also constitute electronic evidence.

ii) Storage Location of Electronic Evidence?

Electronic evidence can be stored in many places. If it is dealing with a business, it can be expected that the business will be using computers, perhaps a network and the Internet. It can be saved on personal PCs, servers, personal and official mobile phones, on backup tapes, USB drives, portable hard drives, off-site mail servers, in remote storage such as Google, Microsoft Sky Drive, Dropbox. [525]

[524] Larry Daniel and Lars Daniel, *"Digital Forensics for legal professionals, 115.*
[525] Ibid.

5.1.7.2 Reference Model

The general E-Discovery process consists of six to eight stages, depending on the particular focus and segmentation. The essential steps are described as follows;

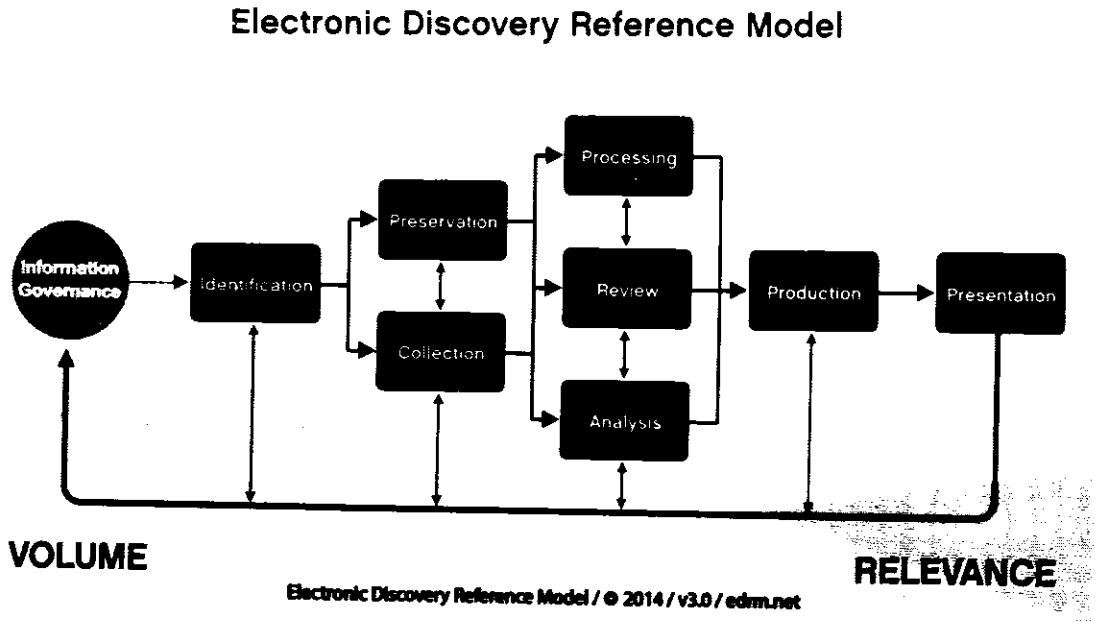

Figure 1 Electronic Discovery Reference Model [526] The steps of the reference model are described below.

5.1.7.3 Steps

The procedure of electronic discovery is not that simple and easy as stated above. It involves a number of steps. The steps of discovery are similar to the above-mentioned model, with little variations in it.

5.1.7.3.1 Information Management

It includes getting electronic house in order. If a litigation management and the digital investigator is organized and has the knowledge of what is located where, and who has

[526] Electronic discovery reference Model, edrm.net. Accessed January 30, 2017. https://pacc-ccap.ca/pacc/wp-content/uploads/2014/06/EDRM-Chart_v3.pdf

control over the information, the task of information management will become much more efficient. [527]

The particulars discussed in the last few sections required to conduct civil electronic discovery are particularly relevant to information management.

5.1.7.3.2 Identification

This process involves the location of potential electronically stored information (ESI) sources. The content and scope, breadth and depth of relevant materials is identified. [528]

5.1.7.3.3 Preservation

This process may involve protection against destruction. Electronically stored information is preserved from a variety of sources, (e.g., tapes, PCs, networks, portable storage devices, etc.) through a number of means. Investigators are not allowed to carry on the investigation process on the originals. So, they preserve it and copy it on some other sources. In this process a digital investigator has to make sure that the data is genuine or the data will lose its integrity in the court. [529]

Preservation of data involves two further steps:

5.1.7.3.3.1 Authentication[530]

Whether it is discovery of civil or a criminal matter, the authenticity and integrity of the evidence is of great importance. To make sure that the evidence is authentic, the digital investigator is supposed to establish "chain of custody". Chain of custody can be maintained by having each person who possesses the evidence sign a receipt for the item, creating a

[527] https://www.edrm.net/frameworks-and-standards/edrm-model/
[528] Ibid
[529] Ibid
[530] See above Chapter 2, para 3.3

"chain". This process may include getting the signature of the original collector, digital forensic analyst, the evidence custodian and the original owner.[531]

5.1.7.3.3.2 Maintenance of Integrity

Maintenance of authentication is not only sufficient, integrity is also important. It is a fact that electronic evidence carries easily alterable magnetic or electronic fields or optical signals. It needs due care and diligence to prove that the evidence is not altered during the stages of collection, storage or review. It can be done through calculation of hash value for each piece of evidence. [532]

5.1.7.3.4 Collection

This involves picking up the required data. The three stages i.e. Identification, collection and preservation in a group comprise of legal processes.

5.2 Criminal Trial: Electronic Evidence

Criminal cases are not usually proven entirely with the help of digital evidence. But they serve to be very strong corroborating evidence. It is not easy to work with the digital evidence at trial, both in civil and criminal cases. However, their presence is a great help in the investigation.

In criminal trials involving electronic evidence, search and seizure is a difficult stage to manage. It has a number of privacy related issues. Also, the fragile nature of electronic evidence poses challenges for the investigation agencies. This section will discuss the problems related to electronic search and seizure in criminal trials.

---

[531] Jack Wiley et. all, *Techno Security's Guide to E-Discovery and Digital Forensics* (Burlington MA: Elsevier, 2007), 36.
[532] Ibid

5.2.1 Importance

Electronic evidence is of great significance in the criminal trial. In this time almost 90 percent of electronic evidence involved in it. Criminals use technology, creating new challenges for the investigation officers, legal officers and judiciary. Large number of drug, child pornography are being done through internet. Technology is increasingly used by the terrorists as well.[533]

There are number of cases in which violent serial offenders have used the Internet to find and lure victims. Increased use of technology also has a positive impact on crime investigation. It has increased the volumes of electronic evidence, which is used to prosecute criminals. For instance, there was a case of a Bind Torture Kill (BTK) serial killer, who sent a floppy to a television station. The digital traces left on a floppy diskette helped investigators to find out that a computer in the church where the serial killer Dennis Lynn Rader was council president, was used.[534]

Computerized records can help establish a sequence of events that may have occurred. Location of a victim, conversations of offenders, call records help a lot in crime investigation.

For example, another murder case was solved, where a father was caught with the help of electronic evidence. Murderer named, Justin Harris, whose son was found dead after being strapped into a hot car for hours. Police searched his computer, where they found out that he made searches similar to the occurred incident. Police reported that Harris used his office PC

[533] United Nations office on Drugs and Crime, *The Use of Internet for Terrorist purposes*, (Vienna: United Nations, 2012), 94.

[534] Police noticed while searching the properties of the document that it was last saved by someone whose name was Dannis. They were able to discover that this floppy was used at Church and Library. Police said that the accused took no stone unturned to delete any identifying information from the disk but he made a fatal mistake of using the disk in church. That is how with the help of electronic evidence a very serious serial killer was arrested. Rebecca J. Rosen, 'The floppy did me in' the story of how police used a floppy disk to catch the BTK killer, The Atlantic daily, January 4, 2014. http://www.theatlantic.com/technology/archive/2014/01/the-floppy-did-me-in/283132/. (Accessed January 30, 2017

to search about "child deaths inside vehicles and what temperature it needs to be for that to occur." [535]

5.2.3 Search and Seizure

The search and seizure of electronic evidence are in most respects the same as any other search and seizure. For instance, as with any general case, the search and seizure of computers or other electronic storage media must be conducted pursuant to a warrant, which is issued by a district court if there is probable cause to believe that they contain evidence of a crime.[536] Issues related to search and seizure are discussed and debated globally, because they involve privacy of many individuals.

A global term "unreasonable search and seizure" has been introduced. It refers to "a search and seizure by a law enforcement officer without a search warrant and without probable cause to believe that evidence of a crime is present". This method is unlawful and unconstitutional in almost majority of the states. A most prominent example of legislation on this subject matter is the Fourth Amendment, of US Constitution. [537] It says;

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue,

---

[535] Michael Pearson. "Georgia toddler death: Who is Justin Ross Harris?" CNN News. June 28, 2014 http://edition.cnn.com/2014/06/26/justice/georgia-toddler-death-father/index.html. (Accessed January 30, 2017)

[536] Yoon & Yang LLC , "Search and Seizure of Electronic Evidence", *Lexology* (December 2015) http://www.lexology.com/library/detail.aspx?g=13704bd6-f4e4-4157-b111-9c58ccfd9f7d (acessed: January 30, 2018)

[537] Other laws dealing with these matters in US are Wire Tap Act, 18 U.S.C. § 2510 (2000), the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (2000), and the Pen Register/Trap & Trace statute, 18 U.S.C. § 3121 (2000).

but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."[538]

A "search" or a "seizure" is reasonable if it meets certain requirements. The first one of them is that the warrant must be issued by a neutral and detached Magistrate Judge. Other requirements are related to officer's conduct, which must be "reasonable," i.e. not in violation of the Fourth Amendment. The officers must stay within the scope of that warrant, or, his actions must be calculated to locate evidence for which the warrant authorizes him to do so. [539]

Most of the states have legislated against unreasonable search and seizure[540] including Pakistan.[541] Courts in the USA are becoming very efficient in analysing the unique nature of digital devices and electronic information and interpreting how the Fourth Amendment would apply to electronic data.[542] In cases where there is an expectation to privacy, law enforcement agencies must obtain a warrant to search from the suitable court in order to carry out search process.

5.2.3.1 Protection Against Unreasonable Search and Seizure

It is the responsibility of the law enforcement agencies to make the search and seizure reasonable. A warrant is a necessary legal requirement before starting search. Large number of US cases have very efficiently tried to define the principles of reasonable search. For

---

[538] U.S Const. amend. IV.

[539] Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39 (2002), 42 (Accessed: March 9, 2017) Available at: http://repository.law.umich.edu/mttlr/vol8/iss1/2

[540] Privacy policy legislations and requirements by country. http://privacypolicies.com/blog/privacy-law-by-country/

[541] Pakistan fair trial Act 2013 (FTA) is a prominent example of curbing unreasonable search and seizure. The FTA 2013 tells the mechanism of application of warrant. Application can only be put by Secret Agencies or Police. It shall be duly signed by the interior minister. Only then High Court Judge can allow for secret warrants permitting digital interception, surveillance, and seizure of equipment. The warrant can only be allowed by a sitting High Court Judge— after a secret hearing 'in chambers.

[542] Dep't of Justice's manual, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, available at http://www.cybercrime.gov/s&smanual2002.pdf.

instance, in case *R v. Jones*[543] the police had the warrant for searching the computer of the accused in the evidence of fraud. So, the computer was seized by the investigation officers. During the course of the investigation, police came across the images which were classified as 'child pornography'. Court decided that the images are not admissible as the police was not entitled to search for child pornography images unless they have obtained a new warrant.

Another case [544] addresses the issue in a different way, where the police sought a warrant to search a house in which it was suspected that marijuana was being grown. In that house they found two computers and a cell phone. The Crown argued that they are entitled to search the computer as the computer comes within the territory of the house.[545]

Similarly, in *Cole* case[546], a teacher gave his laptop to a school board technician to look for a virus which he was entitled to do. When the technician opened the folder, he found a photograph of nude female student, which according to the court was no violation of the right to privacy of the accused. The reason behind this decision is that, such information is rejected where there is an expectation to privacy. Expectation to privacy is lost where the computer, or a phone is handed over to a third party even for technical help. On the other hand, in, *R v. Jones,* [547] the officer was searching the computer for some other reason that is why the images of child pornography were inadmissible.[548]

Since the Fourth Amendment is also a prohibition against those searches and seizures that are unreasonable. The protection of the individual hinges upon what is meant by "unreasonable". The courts say that the question of unreasonableness is relative and each case

---

[543] *R v Jones*, 2011 ONCA 632. Also, in Stephen Mason et al., *"Electronic Evidence"* 2nd edition (Haryana: LexisNexis, 2012), 318.
[544] *R v. Ru*, 2011 BCCA 536.
[545] Infact, one of the computers was logged in to the accused's face book page, and the police were entitled therefore to look at that page. R v. Ru, [2012] SCCA No 94.
[546] *R v. Cole*, [2011] ONCA 218.
[547] *R v Jones*, 2011 ONCA 632
[548] *R v Jones*, 2011 ONCA 632

is to be decided on its own facts and circumstances. [549] The search may be unreasonable if it is out of proportion to the end sought. The term unreasonable cannot, therefore, be precisely defined[550].

The American case law suggests two grounds to consider that whether government's warrantless search of a computer violates rights of privacy of citizens: (1) whether the search violates a reasonable expectation of privacy, and if so, (2) whether the search can be considered reasonable because it falls within an exception to the warrant requirement. [551]

5.2.3.2. Search with Warrant

In a computer forensics case there is an added complexity. The offender is caught red handed if he had evidence in his hand at that time. But the law enforcement agencies cannot arrest him before issuance of warrant. The offender would destroy the evidence while the investigation officer receives the warrant from the court. He can break the laptop or a mobile or he can put lock which is inaccessible by the law enforcement agencies.[552]

There are other issues like such as the contraband might have images of child pornography or drug sales records. This information might be on a laptop, or it might also be on data houses present in other countries. This data might be on a hard drive, or usb etc.

---

[549] Ibid.

[550] Robert F. Bussmann, "Constitutional Law - Protection Against Unreasonable Searches and Seizures", *Marq. L. Rev* 34 no. 52 (1950), 52. http://scholarship.law.marquette.edu/mulr/vol34/iss1/14.

[551] Tara M .Swaminatha,. (2005) "The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defences," *Yale Journal of Law and Technology* 7, no. 1.
http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1017&context=yjolt

[552] Jerry Wegman "Computer forensics: admissibility of evidence in criminal cases." *Journal of Legal, Ethical and Regulatory Issues* 8, no. 1/2 (2005): 3.

Search warrants are bound to be abided by. Investigation officer is strictly prohibited to exceed the authority given. If the data is present in one drive it is not justifiable to seize every computer on the premises.[553]

5.2.3.3 Search Without Warrant

There is a very thin line which differentiates between constitutional and unconstitutional search and seizure. US Department of Justice has published a book, Searching and Seizing Computers and obtaining Electronic Evidence, in which it is stated that the search is constitutional if it does not violate any one's "reasonable" or "legitimate" expectation of privacy. This inquiry they say is based on two discrete questions;

1. Whether the individual's conduct shows "actual expectation of privacy".
2. Whether the individual's subjective privacy expectation is "one that society is prepared to recognize as 'reasonable'". [554]

There is no specific line which indicates the privacy as constitutionally reasonable, for instance US Supreme Court held that there is a reasonable expectation of privacy inside the home, or conversation taking place in the closed phone booth.[555] In contrast, a person does not have a reasonable expectation of privacy where the activities are conducted in open fields. [556]

In order to determine whether the individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer as a closed container such as a briefcase or file cabinet. The basic question, according to the Department of Justice is

---

[553]Ibid.

[554] Katz v. United States, 389 U.S 347, 361 (1967)
[555] Kyllo v. United States, 533 U.S 27, 34-35.
[556] Oliver v. United States, 466 U.S 170, 177 (1984)

whether the person is enjoying a reasonable expectation of privacy in electronically stored on computer or other devices in individual's control. If the answer is "yes" the investigation authorities must obtain a search warrant. [557]

If the computer is openly available, then he would not have the defence of privacy anymore. Similarly, if the computer is freely shared with each other than the individual would have no privacy right. An individual would lose the right to privacy when he hands over the object to the third parties. For instance, a person will have no privacy right, if he handed over the computer or laptop to the technical person for fixation of malfunctioning, etc. [558] In the case of *U.S. v. Simons* [559], a government employee working for the Central Intelligence Agency was suspected of using his office computer to download pornography.

5.2.3.4 Cases Without Warrant Requirement

As a general principle warrant is a mandatory requirement for any search and seizure. But there are certain exceptions to this rule. They are as follows:

5.2.3.4.1 Consent

No warrant is needed when the target consents to a search of his/her computer. Similarly, it is neither required where a third party, such as a spouse, parent, employer or co-worker consent to the search, so long as the third party has equal control over the computer. [560]

---

[557] U.S Government, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations*, (General Books, 2011), Available online at: http://www.cybercrime.gov/s&smanual2002.htm, October 2004 (Accessed: September 1, 2015)., 15.
[558] Ibid.
[559] *206 F.3d 392 (2000)*
[560] U.S Government, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations*, (General Books, 2011), 18.

5.2.3.4.2 Exigent Circumstances

Warrant is not required when probable cause exists, but there is an "emergency", leaving no time or opportunity to obtain a warrant. An example is *U.S. v. David* [561] , where agents observed the target deleting files and immediately seized the computer.

5.2.3.6 Fair Trial Act of Pakistan

The FTA 2013 builds mechanism which allows specific state actors to apply to a High Court Judge for secret warrants for allowing digital interception, surveillance, and seizure of electronic equipment. The warrant can only be granted by a sitting Judge of High Court, after a secret hearing in chambers. The law is applicable to all of citizens of Pakistan including overseas. It also applies to foreign citizens within Pakistan or on board any plane/ship registered in Pakistan; and all transactions or communications originated or concluded within or outside Pakistan. [562]

The main actors under the FTA 2013 are;

1. Intelligence agencies, police and their authorized officers (who apply for a warrant);
2. Minister of Interior (who grants permission for applying to the High Court for a warrant); [563]
3. High Court Judges (who grant a warrant); [564]
4. Service providers (who execute the warrant);
5. Investigation Officers (who investigate offenses the accused is suspected of, based on information collected through warrant);
6. Citizens and foreign nationals affected by the exercise of powers under this Act;

[561] 756 F. Sup. 1385 (1991)
[562] Pakistan Fair Trial Act, § 2.
[563] Pakistan Fair Trial Act, § 6.
[564] Pakistan Fair Trial Act, § 8.

7. Review Committee (composed of Federal Ministers of Defense, Law and Interior). [565]

The warrants for surveillance and interception is initiated by the applicant which includes an officer not below the rank of BPS 20. It will be presented to the interior minister for approval. After approval the application shall be capable of presenting before sitting Judge of High court who will approve it and then the internet service provider shall be authorized to intercept conversation of the suspect. For interception of a phone call for surveillance of unusual activities, assent of responsible authorities would have been enough. [566]

In Pakistan's context when normal procedures are very slow, involving an interior minister and sitting High Court judge has made the procedure very complicated and mission impossible.

In the previous sections, it was observed that in USA a magistrate shall issue a search warrant where necessary but Pakistan's law is complicated. In these sensitive issues, approaching the interior ministers and getting their signatures is not an easy job. In Pakistan's scenario, it is not easy to locate the interior ministers in their offices. Here normal official works take longer than usual. And if in these matters, ministers are involved, the matter become a victim of delay. Ministers are the top ranked officers who are busy with other political duties as well. States throughout the world are making their procedures easy and speedy. But the situation is totally different in Pakistan. Here instead of making thing easy, procedures are subjected to more difficulties in which a cyber-criminal can escape.

Cyber-crimes are so fast that they can rob everything, or effect the critical infrastructure in fraction of seconds but here in Pakistan the authorities will be running for minister's signature at that time.

---

[565] Waqqas Mir & Hassan Niazi, Surveillance Laws and Practices In Pakistan: History, Current Legislation And Lessons From The United Kingdom.
[566] Pakistan Fair Trial Act, § 2, 6 and 8.

5.2.3.7 Pakistani Cyber Law

Warrants for search and seizure is a legal requirement. Section 33 of Prevention of Electronic Crimes Act speaks about the procedure of seeking a search warrant. It states;

> **"33. Warrant for search or seizure. —**
>
> (1) Upon an application by an authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that
>
> 1. May reasonably be required for the purpose of a criminal investigation, criminal proceeding which may be material as evidence in proving a specifically identified offense made out under this Act; or
> 2. Has been acquired by a person as a result of the commission of an offense, the Court may issue a warrant, which shall authorize an officer of the investigation agency, with such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium relevant to the offense identified in the application and access, seize or similarly secure any information system, data, device or other articles relevant to the offense identified in the application.
>
> (2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss of data, information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazetted officer of the investigation agency, may enter the specified place and search the premises and any information system, data, device or other articles relevant to the offence and access, seize or similarly secure any information system, data, device or other articles relevant to the offence:
>
> Provided that the authorized officer shall immediately, but not later than twenty-four hours bring to the notice of the Court, the fact of such search or seizure and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case."

Section 43 states about the non-cognizable nature of offenses as follows;

> **"43. Offenses to be compoundable and non-cognizable. —**
>
> (1) All offenses under this Act, except the offenses under sections 10, 21 and 22 and abetment thereof, shall be non-cognizable, bailable and compoundable: Provided that offenses under section 17 shall be cognizable by the investigation agency on a written complaint by the Authority.[567]
>
> (2) Offenses under sections 10, 21 and 22 and abetment thereof shall be non-bailable, non-compoundable and cognizable by the investigation agency"

According to section 34, it is a legal requirement to get a search warrant before starting any search process. The problem is that according to PECA, all the offences are non-

[567] Section 10, 21 and 22 are related to cyber terrorism, offences against modesty of natural persons and child pornography respectively.

cognizable. It means that the police officer does not have authority to arrest and present before the court without receiving search warrant.

This way, if the investigation officer finds a mobile phone in the hands of the criminal, he cannot arrest that person red handed or seize the mobile phone before getting warrants. When the officer will go for getting warrant the offender will destroy the evidence or lock the mobile phone which cannot be unlocked later.[568] Laptops, hard drives, USBs, mobiles are so fragile in nature that if they are broken or thrown away the investigation agencies will not be able to recover most important pieces of evidence or data against the accused.

Such situations must be carefully handled by the legislatures and efficient laws must be passed so that such situations may not arise. As stated, earlier warrants are a requirement where there is an expectation to privacy. But if a person is doing an offense, he must be caught on the spot. For instance, in the USA's laws, there should be exceptions to the rule of warrant for exigent circumstances. The places where the accused have the knowledge that the law enforcement agencies are going to catch him, he should be arrested on the spot, even before warrant. Because there is a danger that he will destroy the evidence.

Indian Information Technology Act has also legislated in the same way. In it, all the offences which have 3 years' imprisonment or more are cognizable. According to the §. 77 of IT Act, 2000 "notwithstanding anything contained in the code of criminal procedure, 1973 (2 0f 1974), the offense punishable imprisonment of three years and

[568] Now a days apple mobile companies have declared that they have encrypted the codes of mobile in such a way that they can not be unlocked even by the company. Recently in Ayan Ali (model) case her mobile phone was sent in many countries but they could not be unlocked. Such mobile phones can be unlocked by restore factory settings but the evidence is not complete.

above shall be cognizable and the offenses punishable with imprisonment of three years shall be bail able."[569]

We have examples from laws of other countries such as USA and Canada. Wherever, there is a chance of destruction of proof or evidence, the offences are cognizable. Another very serious issue here lies with the cognizable nature of offences in PECA which upsets the whole system of catching the criminals. The cyber criminals come and rob everything, but investigation officer cannot arrest them unless they do not have any search warrant with them.

5.3 Conclusion

Electronic data is a fast-growing field, which needs to be handled and managed properly. Practically pursuing the case, involving electronic evidence, in court of law is a harder than the admissibility phase. Electronic Evidence operates differently in civil and criminal law. In civil law the challenging task is the procedure of electronic discovery. In criminal cases on the other hand is the procedure of search and seizure. It involves privacy of individuals as well as institutions.

Electronic evidence is lengthy technical process which requires a complete collaboration of IT bodies, management of institution and legal experts. Electronic discovery can be fatal to the reputation of institution and it can be very costly, if it the electronic data is not archived in an effective manner. The management, IT and legal experts of a firm need to make policies for keeping the data save and accessible. Otherwise, serious sanctions can be imposed on them.

Cloud computing is a proposed solution to the problems of electronic discovery.

---

[569] Indian IT Act 2000, § 77.

Electronic evidence in criminal trials is also not that easy. The privacy of citizens is to be taken care of, during the process of search and seizure. The information seized if contain privileged information is not admissible. Search without warrant is also strictly not allowed unless made in exigent circumstances.

The procedure followed in Pakistan for issuance of warrant in order to allow digital interception, surveillance, and seizure of electronic equipment is very difficult. The application needs to be initiated by a High Court judge, which further needs ascent from interior minister. This law is problematic.

PART 2

CHAPTER 6

LAW ELECTRONIC EVIDENCE AND COMMERCIAL TRANSACTIONS IN PAKISTAN'S LEGAL SYSTEM

6.1 Introduction

The enormous growth of electronic data, both in the public and private sector, has resulted in the evolution of electronic evidence as a fundamental pillar of all major fields of communication, processing and documentation. Various forms of electronic evidence are being used increasingly in civil and criminal litigations. During trials, Judges are often asked to rule on the admissibility of electronic evidence which substantially impacts the outcome of a civil lawsuit or the conviction/acquittal of the accused.[570]

Currently, the legal scenario of Pakistan regarding electronic evidence is in a very immature state. The laws in Pakistan curbing cyber-crime and crimes related to cyber security are not in par with the international standards. There are a large number of official and non-official websites and critical infrastructures which have been compromised due to cybercrimes. It is a crucial demand of time to establish cyber laws and harness the situation. The few cyber laws that do exist are not fully updated. [571] There is a need to align them with the demands of time.

6.2 Admissibility of Electronic Evidence in Pakistani Law

This chapter is going to explore the status of Pakistani legal system on the areas which have been covered previously in Islamic law and Western law. For instance, relevance, authentication, hearsay, original writing rule, electronic discovery, electronic search and seizure and documentary evidence etc.

6.2.1. Admissibility of electronic evidence in Pakistani law.

Electronic Documents

[570] These types of problems are already discussed in the topics 3.4.6.
http://www.neerajaarora.com/admissibility-of-electronic-evidence-challenges-for-legal-fraternity/
[571] For instance. Electronic Transaction Act 2002, Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes 206.

Documentary evidence is the one which is produced in the form of paper or something which has a physical existence. But as mentioned above that technology has widened the scope o documentary evidence to a great extent. For instance, Article 2(b) of Qanun-e-Shahadat Order, 1984 mentions a long list of documents which were not in the definition of documentary evidence few decades ago. For instance, it says, "A document means any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means intended to be used or which may be used for the purpose of recording of matter." [572]

Similarly, Section 2(c) of Qanun-e-Shahadat Order while defining "evidence" includes documentary evidence in its definition. It says;

> "Evidence includes;
> (i) All statements which the Court permits or requires be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; and
> (ii) All documents produced for the inspection of the Court; such documents are called documentary evidence."

Electronic Evidence is expressly added in the definition of documentary evidence in Pakistani law in Article 164 of Qanun-e-Shahadat Order 1984. It affirms the admissibility of electronic documents in courts as;

> "164. Production of evidence that has become available because of modern devices, etc.: In such cases as the Court may consider appropriate, the Court may allow to be produced any evidence that may have become available because of modern devices or techniques."

> Section 27-B of Anti-terrorism Act 1997 says;
> "27-B. Conviction on the basis of electronic or forensic evidence etc.
> Notwithstanding anything contained in this Act or Qanun-e-Shahadat, 1984 or any other law for the time being in force, a person accused of an offence under this Act may be convicted on the bass of electronic or forensic evidence or such other evidence that may have become available because of modern devices or techniques referred to in Article 164 of the Qanun-e-Shahadat, 1984."

Above mentioned two sections open the door of electronic documents as admissible evidence. courts cannot deny acceptance of any proof solely on the ground that it is from modern means. This stance has been very excessively endorsed by a large number of Pakistani judgments which not

[572] QSO article 2(b)

only admits electronic record as docuemtary evidence but it also considers it as a very strong mean of proof which is undeniable. as After mentioning the above-mentioned statutes in a judgment it was observed by the court in, Sikandar Ali Lashari v. State that:[573]

> "8. After analysing and dissecting the aforesaid provisions of different statutes, we reach to the final that the definition of document is much expanded and any substance by means of letter, figures or marks is document including an inscription on a metal plate. It is quite clear from the definition of CD that it is made by polycarbonate with one or more metal layers capable of storing digital information and audio and visual data is recorded as a series of metallic pits enclosed in PVC. So far as USB (Universal Serial Bus) flash drive is concerned, it is often used for the same purposes for which floppy disks or CDs are used, i.e., for storage, data back-up and transfer of computer files. it is immune to electromagnetic interference (unlike floppy disks), and are unharmed by surface scratches (unlike CDs). The data which may be transferred on CD may also be stored /transferred on USB drives so it is only a medium and vehicle of storage that's why in our view the data stored on CD and USB flash drive is covered in the wide-spread definition of document."

It was observed by the said court that the meaning of the word 'document' in PPC and QSO is generic and it includes words printed on a paper, photographs and other things irrespective of the mode of production of document.

In Salman Ahmad Khan v. Judge Family Court, [574] Multan case court permitted the applicant to record her statement through a video link. The court held that recording of evidence through modern devices is permissible under article 164 of Qanun-e-Shahadat Order.

In another case Asfandyar v. Kamran, [575] it was observed by the court that CCTV footage is admissible in a preview of article 164. But "mere production of CCTV footage as a piece of evidence in court was not sufficient to rely upon the same unless and until it was proved to be genuine. In order to prove the genuineness of such footage it was incumbent upon the defence or prosecution to examine the person who prepared such footage from the CCTV system" the court said;

---

[573] 2016 YLR 62 KARACHI-HIGH-COURT-SINDH
[574] 2017 PLD 698 LAHORE-HIGH-COURT-LAHORE.
[575] 2016 SCMR 2084 SUPREME-COURT.

Similar case like, Amar Yasir Ali v. State[576] in this case ground for refusal of CCTV footage were discussed by the court. It was observed that "CCTV footage being played in open court is not a sufficient evidence to be relied upon, unless corroborated and proved to be genuine. Court observed that it is incumbent upon prosecution to examine the person who recorded video to testify the same. The prosecution failed to identify the source of CCTV video. Investigation officer who received the video disclosed that it was handed over to him by a person who was not interested in disclosing his name and identity. It was observed by the court that such evidence is not admissible in court."

In another case Munas Parveen v. Additional sessions Judge/Ex-officio Justice of Peace, Shorkot, [577] it was observed by the court that "information conveyed over modern devices such as SMS---Such information was means of communication validly accepted all over the world however the witness in whose presence such information was conveyed or received was always important to prove a fact through its verification—Although under Art 73 of Qanun-e-shahadat, 1984 modern devices were legally acceptable yet in order to prove a fact the required procedure had to be followed."

6.2.7.1 Audio Tape Recordings

Admissibility of a tape recording is no longer a grey area in Pakistan. The courts in Pakistan admitted tape recordings as a relevant fact. It was observed in the case Kashif Anwar v. Aga Khan University[578] when the appellant, being a medical student of the fourth year, challenged the admissibility of tape-recordings. The brief facts of the case are that Kashif was a student of the 3rd year in medical college at the Agha Khan University. In an evening of September, 2004, the plaintiff along with some other 4th year students met to celebrate their end of examination party.

[576] 2013 PCrLJ 783 KARACHI-HIGH-COURT-SINDH
[577] 2015 PLD 231 LAHORE-HIGH-COURT-LAHORE
[578] 2013 YLR 2294 Karachi-High-Court-Sindh

After driving for a while, they returned to the campus. While partying, they used drugs. Unfortunately, one of the students had a fatal reaction to drugs and died the next day. The family of the deceased filed an FIR and plaintiff was one of the accused. By the decision of the disciplinary committee the plaintiff was rusticated from the University. The reason given was he was guilty of aiding, abetting and possession of the prohibited drugs in the vicinity of the University. The rustication orders were given by the disciplinary committee of the University. The plaintiff sued the dean of the committee. In suit he pleaded that he was wrongfully rusticated. Plaintiff raised objections that he was not given a chance to defend himself in front of the disciplinary committee. As a result, three audio tapes were submitted as evidence in the court by the defendant. Plaintiff raised issues that the audio tapes were not admissible as they were not properly authenticated and they are tampered with. He further pleaded that the material evidence which was in favour of plaintiff was concealed. The plaintiff asked for the complete recording of disciplinary committee, which he could get checked by an expert. Therefore, 8 more audio tapes were submitted in court. In this case the recordings were not handed over to the plaintiff deliberately to get an expert witness. The evidence given to the plaintiff was not the master copy and plaintiff asked for the master copy of expert testimony which was denied by the defendant.

The Supreme Court in this judgment gave some golden principles for admissibility of audio tapes:

It was observed by the court that a principle for admissibility is "Best evidence rule" and "rule against hearsay" is that the document can, only be produced in evidence by the maker and in case of tape-recording this principle has been interpreted to mean the tapes can be admitted in evidence if they are produced by the one who recorded them and that particular person must be in a position to identify the voice recorded in that tape.

In the said case, Supreme Court observed that in order to remove the objections from the admissibility, it was imperative for AKU to have the tapes played and identified by the person who was responsible for the recordings. But it was not done.

The court observed that the audio tapes were also inadmissible because there was lack of application of any security procedure to them for protection against tampering in terms of Art. 78 A of the Qanūn-e-Shahādat, 1984, which says that "if an electronic document is alleged to be signed or generated wholly or in part by any person, through the use of an information system, and such allegation is denied, the application of a security procedure for the electronic document has to be proved." This security procedure as prescribed by Sec 2 (x) of the Electronic Transaction Ordinance, 2002 states that; x) Security Procedure means a procedure which is:

> "i) Agreed between parties;
> ii) Implemented in the normal course by a business and which is reasonably secure and reliable; or
> iii) In relation to a certificate issued by a certification service provider, is specified in its certification practice statement; for establishing the authenticity or integrity, or both, of any electronic document which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices."

The court observed that in the present case, sub clause 1 was applicable since plaintiff had denied the authenticity of the tape-recording of his statement. It was imperative for AKU to have shown application of the above security procedure to the tapes prior to admitting them into evidence. But AKU failed to comply with this condition. Even AKU could not succeed in breaking the security tabs to prevent eraser, or re-recording, which is a very basic precaution that can be taken to prevent any tampering. Court observed that circumstantial evidence shows that the chain of custody of those audio tapes was not proved well. This judgment discussed Indian judgment as precedent;

> "67. In Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra (AIR 1975 Sc 1788), the Supreme Court of India prescribed the following pre-conditions for the admissibility of tape-recording as evidence: --
>
> a) The voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who know it.
> b) The accuracy of that was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstantial had to be there so as to rule out the possibilities of tampering with the record.
> c) The subject-matter recorded had to be shown to be relevant according to rules of relevancy found in the Evidence Act."

The court held that the audio tapes given in evidence were not properly authenticated and thus not admissible. Therefore, the court held that the degree to the student should be conferred and his rustication orders must be cancelled.

6.2.2. Relevance

Article 2(3) of Qanun-e-shahadat order 1964 states about the relevancy of facts;

> "(2) One fact is said to be relevant to another when the one is connected with the other in any of the ways referred to in the provisions of the Order relating to the relevancy of facts."

Section 46-A of Qanun-d-Shahadat Order states that the information is relevant if it is generated from an automated information system.

> "*46-A. Relevance of information generated, received or recorded by Automated system.* —Statements in the form of electronic documents generated, received or recorded by an automated information system while it is in working order, are relevant facts.[579]

Relevance is a matter of common sense for the judge. If the facts are so closely connected to each other that one fact cannot be proved without the other then it is called a relevant fact.[580]

Qanun-e-Shahadat order is not directly addressing the relevance of electronic evidence other than in Article 46-A. Where relevance of fact is connected to an automated information system while in working order.

The problem lies here is that at one place it is stated that when facts are so closely connected to each other they are relevant. While in 46-A it is stated that only those statements are relevant which are generated from an automated information system. It is a fact that electronic evidence does not comprise only of information which is derived from an

---

[579] Qanun-e-Shahadat Order Article 46 Inserted By ETO

[580] See above chap 3, para 3.3.

automated information system. It also deals with a number of other sources like, computer stored information, servers, clouds etc. Pakistani law is silent on the information which is stored on a computer. It means that information is not relevant.

6.2.2. Authentication

Authentication of electronic evidence means the data is trust-worthy.[581] It is a most important stage for admissibility. Methods of authentication are very well elaborated in western law as well as English Law. Pakistani law also deals with authentication of electronic evidence in a few sections. For instance, section 5 of ETO states;

> "1) The requirement under any law for any document, record, information, communication or transaction to be presented or retained in its original form shall be deemed satisfied by presenting or retaining the same if:
> (a) There exists a reliable assurance as to the integrity thereof from the time when it was first generated in its final form; and (b) it is required that the presentation thereof is capable of being displayed in a legible form.
> (2) For the purposes of clause (a) of sub-section (1);
> (a) the criterion for assessing the integrity of the document, record, information, communication or transaction is whether the same has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display ; and (b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the document, record, information, communication or transaction was generated and all other relevant circumstances. "

The above-mentioned section is a part of Electronic Transaction Ordinance. It talks about authentication of electronic evidence.[582] Clause 1 mentions that documents or communication is considered original if there is a reliable surety about its integrity. It means that when it was generated for the first time, after that time there must be surety that since then it is under safe custody. But how will it be judged that it assures integrity? Fragile nature of electronic evidence suggests that it can be altered very easily. It would have been better if it was mentioned that how will the integrity ensured. For instance, if hash values are generated form a document then

---

[581] See above Chap. 3, para 3.4.
[582] Chapter 3. Para 3.4 shows that authentication of electronic evidence is a very vast topic and needs proper legislation, but above-mentioned section of ETO deals with it in quite a lighter note.

it is very easy to check whether the document ensures integrity or not. [583] the same thing is asserted in subclause 2 while discussing the criteria of integrity. It also says the same thing i.e. the document should be complete and unaltered. But no method or way is mentioned here how will it be proved. This vagueness in law may cause certain ambiguities for the citizens who seek justice. And such scenario can cause in to misleading situation for judges and lawyers. Such lacunas must be curtailed from law.

It is to be noted that subsection 2, clause b mentions that the ascertainment of integrity of electronic evidence shall vary according to type of document. It has mentioned different types of documents i.e, communication, transactions, record and information. But it has not differentiated between computer stored and computer-generated evidence. Likewise, it has not mentioned hearsay rule regarding computer stored evidence. It has been mentioned that the document has remained complete and unaltered, apart from the changes arising in the normal course of communication, storage or display. This section does not define what the course of communication is. The method of proving a document incomplete and unaltered remains ambiguous.

For authentication, idea of electronic information being complete and unaltered makes sense for computer-generated evidence. [584] But if the information in a computer stored evidence[585], this idea cannot be justified. The reason behind, is that it is manually stored in a computer. One of Pakistani judgment explains the meaning of complete and unaltered electronic information in case there is an addition in the instrument. *Alamgir Khalid Chughtai v. State*[586]states;

> "Calculation is available, as the call receiving has no physical existence, but it was available on the computer. All the detail of telephone number, including an I.P.....The learned counsel for the appellant has contended that the documents were not proved in accordance with Qunun-e-Shahadat, 1984 and were not admissible in evidence, but in my view Section 3 of Electronic transactions Ordinance, 2002 is the complete answer.... No doubt that criterion for assessing

[583] IT Act of India mentions hash values.
[584] See above chap. 3, para 3.4.4.1.
[585] See above chap. 3, para 3.4.4.2.
[586] 2009 PLD 254 Lahore-High-Court-Lahore

the admissibility, of the document or information, etc. is that the same should remain complete and un-altered but at the same time it is also provided in the above quoted law that if there is any addition in instrument, and that arise in normal course, and the document is still complete and un-altered that could not be brushed aside."

Electronic data changes rapidly even without the knowledge of an ordinary computer user. If a document is saved from one place to another the Meta Data of that particular document changes. So the method of ascertaining that this document is unaltered and complete is not defined. Authentication of electronic evidence means it is unaltered and complete. The method of ascertaining authentication still remains a grey area.

Such problems are addressed in the laws of other countries. For instance, in the USA's law of evidence, they have clearly mentioned that they would assess the integrity of a document with the help of hash values. In US codes, Code no. 44926, it is clearly mentioned that the document shall be maintained and secured by encryption and hashing.[587] Such rules of procedure should be absorbed in the ETO as well so that the chances of confusion may be avoided among the judges as well as the lawyers.

Challenges of reliability and admissibility are raised if the document is not protected by technological measures.[588] Electronic Transaction Ordinance is silent about ascertaining the reliability of data. In this age of high-end technology and cyber-crimes, a state cannot afford a silent law on this delicate issue which can cost millions to the institutions.

Section 46-A discusses the integrity of the information system. The criteria for authentication of a document generated by an automated information system is defined as "in working order". The meaning of working order is unexplained and remains ambiguous. The law is silent about the methods of checking working order of an information system. All these factors lead to uncertain statements about the authentication of electronic documents.

---

[587] https://www.law.cornell.edu/uscode/text/49/44926

[588] http://www.supremecourt.gov.pk/ijc/articles/10/3.pdf p. 12

Pakistani law is silent about different means of authentication as well. Both Islamic and western law has well-elaborated status different means of proof. Like, authentication through oral testimony, circumstantial evidence, documentary evidence, expert testimony etc. Pakistani law is also silent about the authentication of e-evidence through Metadata, hashtags or any other technology which are the most helpful tools for authentication of electronic evidence.

6.2.3. Hearsay

The Rule against hearsay in Pakistani regarding electronic evidence is an area unaddressed. If a computer stored evidence is hearsay, a method of its in Pakistani law is still a grey area. Although the situation is completely opposite in case of Western law[589]. Islamic law also deals with the problem of hearsay though not specifically with electronic evidence. [590]

6.2.4. Original writing rule

The original writing rule in Pakistani law has changed like the laws of other western countries.[591] This rule has been abolished in Pakistan as well. Section 4 of the Electronic Transaction Ordinance (ETO) deals with original writirg rule and says;

> "4. **Requirement for writing.** —The requirement under any law for any document, record, information, communication or transaction to be in written form shall be deemed satisfied where the document, record, information, communication or transaction is in electronic form, if the same is accessible so as to be usable for subsequent reference."

It has been mentioned in section 4 of ETO that the requirement to be written shall be satisfied if it is in electronic form and is available for future reference. But it does not directly address the issues of original writing.[592] It does not talk about the integrity of system i.e if the document is generatcd from an electronic system, integrity of which is proved beyond doubt shall be considered original whether it is generated numerous times. All the

---

[589] See above chap. 4, para. 4.2.
[590] See above chap. 2, para. 2.3.3.14
[591] See above chap. 4, para. 4.3.1.
[592] Para 4.3.1 clearly mentions legislations talking about original writing rule in legislation of Canada.

copies shall be considered as original. This idea is discussed further under article 73 of Qanun-e-Shahadat Order 1964 as;

> **"73. Primary evidence:** "Primary evidence" means the document itself produced for the inspection of the Court.
>
> Explanation 2: Where a number of documents are all made by one uniform process, as in the case of printing, Lithography or photography, **each is primary evidence of the contents of the rest**; but where they are all copies of a common original, they are not primary evidence of the contents of the original
> [Explanation 3: A printout or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic from if the automated information system was in working order at all material times and, for the purposes hereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material times.
> [Explanation 4.- A printout or other form of reproduction of an electronic document, other than a document mentioned in Explanation 3 above, first generated, sent received or stored in electronic form, shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored.]"

Section 73 mentioned above highlights the concept of primary evidence in case of electronic evidence. In case of physical documents, primary evidence is usually one which is the original copy of the document. But the case is different in electronic evidence where all the documents produced through a uniform process like printing, lithography are all primary evidence. Even the printout or other output of automated system shall be primary evidence. But there are two pre requisites for considering a printout admissible. First one of them is that information system is in working order, secondly if a security procedure. [593] The condition of information system being in working order is ambiguous. It is related to the condition of admissibility of business record in which the data generated from automated system is taken from the data base which is being relied during the course of ordinary business. [594] but this was supposed to have been mentioned in this

---

[593] Section 2 sub clause (x) of ETO 2002 defines "security procedure" as; it means a procedure which:
(i) is agreed between parties; (ii) is implemented in the normal course by a business and which is reasonably secure and reliable ; or (iii) in relation to a certificate issued by a certification service provider, is specified in its certification practice statement; for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices;

[594] The reason for the presumption of accuracy of business record is that business relies on certain records in day to day transaction which develop a certain level of trustworthiness. [594] Secondly, as a normal course of a business, the employees are under an obligation to record, observe and report the facts correctly. Stephen Mason et al., *"Electronic Evidence"* 2nd edition (Haryana: LexisNexis, 2012), 256.

section. The second condition of applying the security procedure for authentication of electronic evidence is also very effective and it mentions the technical methods of authentication like hash values and electronic signatures etc.

So the above mentioned sections shed light on the abolition of original writing rule on electronic evidence and section 73 talks about change in primary evidence in case of electronic evidence. but the detail of working order of automated system are missing. Which can create confusions. This is the responsibility of judiciary to further explain the meaning and implication of this word "working order".

6.2.4. Electronic Discovery

The laws that are followed in Pakistani law for dealing with Electronic Discovery are the ones which deal with general document discovery. These are section 94 of Cr. Pc. It says;

> **"94. Summons to produce document or other thing.**-(1) Whenever any Court, or 1* * *, any officer in charge of a police-station considers that the production of any document or other thing is necessary or desirable for the purposes of ,any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it or to produce it, at the time and place stated in the summons or order"

The above-mentioned section deals with physical document discovery. The most important issue of electronic discovery is totally absent from Pakistani law. Today most of the cyber cases involve electronic discovery. So, this area must have proper legislation.

Section 30 of CPC deals with document discovery in CPC has the same problem. It does not address electronic discovery. There is no updated legislation in Pakistan which deal with the highly developed area of electronic discovery.

> **"30. Power to order discovery and the like:** Subject to such conditions and limitations as may be prescribed, the Court may, at any time, either of its own motion or on the application of any party: -

(a) make such orders as may be necessary or reasonable in all matters relating to the delivery and answering of interrogatories, the admission of documents and facts, and the discovery, inspection, production, impounding and return of documents or other material objects producible as evidence;
(b) Issue summonses to persons whose attendance is required either to give evidence or to produce documents or such other objects as aforesaid;
(c) Order any fact to be proved by affidavit."[595]

Electronic Discovery[596] is discussed in detail in chapter 5. There are no doubts about its importance in daily litigation. The prime importance of the electronic discovery is evidence from the fact that almost two third of modern-day law suits comprise of electronic discovery. In Pakistan the ratio is not that high but it is not doubtful that it will be even higher in near future. As the use of technology is rampant in society. Keeping these facts in mind Pakistan must legislate accordingly in order to cope with any alarming situation. After passing through cases of Khanani and Kalia where the accused were acquitted due to lack of relevant laws. In Axact case the situation was no different. As lack of laws means tools are absent to punish. The above-mentioned section pertains to discovery of physical documents only and not electronic discovery. Which is nto less than an alarming situation in this modern age. Electronic discovery requires special legislation and policies.

6.2.5. Search and Seizure

Sections like 102 also deal with the search but not dealing with electronic search. For instance, section 102 of Cr. Pc

> **"102. Persons in charge of closed place to allow search.**-(1) Whenever any place liable to search or inspection under this chapter is dosed, any person residing in, or being in charge of such place shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein."
>
> **103. Search to be made in presence of witnesses.**-(1) Before making a search under this chapter, the officer or other person about to make it shall call upon two or more respectable inhabitants of the locality in which the place to be searched is situate to attend and witness the search 1[and may issue an order in writing to them or any of them so to do].

---

[595] Civil Procedure Code § 30.
[596] Chapter 5, para 5.1

(2) The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person signed by such witnesses; but no person witnessing a search under this section shall be required to attend the Court as a witness of the search unless specially summoned by it.
(3) Occupant of place searched may attend. The occupant of the place searched, or some person in this behalf, shall, in every instance, be permitted to attend during the search, and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person at his request.
(4) When any person is searched under section 102, sub-section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person, at his request.[597]

N.A.O 1999- 19 (e) deals with issue of surveillance. It says;

"[(e) where there is a reasonable suspicion that any person is involved in or is privy to an offence under this Ordinance, the Chairman NAB may, with the prior approval in writing of the High Court concerned, direct the surveillance of that person may be carried out through such means as may be necessary in the facts and circumstances of the case and the Chairman NAB, may in this regard seek the aid and assistance of any 2 [Governmental] agency and the ir formation so collected may be used as evidence in the trial under this Ordinance. Provided that the copies obtained or information received or evidence collected under clauses (d) and (e) shall be 3 [kept] confidential and shall not be used for any purpose other than for legal proceedings under this Ordinance.]" [598]

It is a matter of a fact that in case of exigent circumstances bail application can be refused if there is any danger to the evidence. Same was the case of *Adnaan Hafeez v. the State*, when bail was refused on the ground that if bail is granted to the petitioner, he will tamper or even destroy the evidence. Petitioner being a technical expert, is a mastermind of the gang who has been hacking I.Ds of various travel agents.

On the other hand, bail was granted to the applicant in case of *Hassan Sameer and another v. The state* because reliance was placed on the documentary evidence which was already in possession of the prosecution. The applicant was unable to tamper the evidence.

[597] Criminal Procedure Code § 102.
[598] N.A.O 1999 § 19 sub sec (e)

6.2.6 Oral evidence

Oral evidence means and includes all statements that the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry.[599] 'Oral' ordinarily means 'words spoken by mouth'.

> **"70. Proof of facts by oral evidence:** All facts, except the contents of documents, may be proved by oral evidence.
> **71. Oral evidence must be direct:** Oral evidence must, in all cases whatever be direct, that is to say—
> If it refers to a fact, which could be seen, it must be the evidence of a witness who says he saw it;
> If it refers to a fact, which could be heard, it must be the evidence of a witness who says he heard it;
> If it refers to a fact, which could be perceived by any other sense or in any other manner, it must be the evidence of a witness who says he perceived it by that sense or in that manner;
> If it refers to an opinion or to the grounds on which that opinion is held, it must be the evidence of the person who holds that opinion on those grounds:
> Provided that the opinions of experts expressed in any treaties commonly offered for sale and the grounds on which such opinions are held, maybe proved by the production of such treaties if the author is dead, or cannot be found, or has become incapable of giving evidence, or cannot be called as a witness without an amount of delay or expense which the Court regards as unreasonable:
> Provided further that, if oral evidence refers to the existence or condition of any material thing other than a document, the Court may, if it thinks fit, require the production of such material thing for its inspection:
> Provided further that, if a witness is dead, or cannot be found or has become incapable of giving evidence, or his attendance cannot be procured without an amount of delay or expense which under the circumstances of the case the Court regards as unreasonable, a party shall have the right to produce, "shahada ala al-*Shahādah*" by which a witness can appoint two witnesses to depose on his behalf, except in the case of Hudood." [600]

There has been no any amendment in Qanun-e-Shahadat Order regarding the admissibility of oral testimony in the context of electronic evidence. But Western and India laws and cases available on this matter. For instance, the evidence Act provides that oral admissions as to the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.[601] Another American judgment is setting out criteria for testimony in of electronic records in form of data stored on magnetic tapes in the case of *King v. State of Mississippi or Use and*

---

[599] QSO sec 2 § (c).
[600] Ibid article 70 and 71
[601] Section 119, Indian Evidence Act.

Benefit of Murdock Acceptance Corporation[602] Print-out sheets of a business record stored on magnetic tapes were admissible in evidence is showed:

'(1) that the electronic computing equipment is recognized as standard equipment, (2) the entries are made in the regular course of a business at or reasonable near the time of the happening of the event recorded, (3) the foundation testimony satisfies the court that the sources of information, method and time of preparation were such as to indicate its trust worthiness and justify its admission.'[603]

Present thesis has discussed at length the rule regarding admissibility of oral testimony in Islamic law and then admissibility of oral testimony regarding electronic evidence in western law[604]. Section 70 and 71 does not come in coherence with both. First of all, there was supposed to have been mentioned that the criteria for admissibility of evidence for physical and electronic evidence shall be so and so. [605] secondly there was supposed to have mentioned the situation where witness is not required i.e. computer-generated evidence. in that situation the circumstantial evidence prove that the automated system is reliable and hence proof can be admitted without testimony. Shahadah ala shahadah also has certain conditions for admissibility in Islamic law. such conditions must be mentioned here in QSO as well.

6.2.8 Expert Testimony

Law of Pakistan expressly provides admissibility of expert testimony specifically about electronic evidence. Article 59 of the Qanun-e-Shahadat order states;

> **"59. Opinions of experts·** When the Court has to form an opinion upon a point of foreign law, or of science/or art, or as to identity Of hand-writing or finger impressions, 1[or as to

---

[602] Miss. m 222 So. 2d 393.

[603] Miss. m 222 So. 2d 393 at [9]. See United States of America v Weather spoon. 581 F.2d 595 (7th Cir. 1978) and Rosenberg v Collins, 624 F. 2d 659 (1980), where sufficient testimonial evidence was adduced ot lay the foundation fr the admission of computer printout.

[604] Chapter 3 para----------

[605] That the witness must have a just character. And that the process of screening of witness must take place before presenting testimony in court. there must not be any blood relation or business partnership between the witness and party. Chap 2 para -----

authenticity and integrity of electronic documents made by or through an information system shall be inserted; and] the opinions upon that point of persons specially skilled in such foreign law science or art, or in questions as to identity of hand-writing or finger impressions are 1[or, as to the function specification, programming and operation of information system are relevant facts.] Such persons are called experts.

60. Facts bearing upon opinions of experts: Facts not otherwise relevant, are relevant if they support or are inconsistent with the opinions of experts, when such opinion is relevant."

Section 59 of Qanun-e-Shahadat Order tell about the admissibility of expert testimony. Electronic evidence is also included in it. But law is silent on what should be the criteria of qualification of expert testimony. It is elaborated further by judgments. The status of expert testimony is discussed in, *Fida Muhammad and another v. Umar Khattab,* [606] it was observed by the court that expert testimony is a circumstantial evidence in nature. Circumstantial evidence, is weak evidence in absence of direct evidence. Unless expert evidence is corroborated by other strong evidence. If the expert is not cross-examined in court it loses its credibility. In another case *"Allah Dino and two others case"*[607] an expert report which was not examined by the court was rendered inadmissible by the Honourable Supreme Court.

Qualification of experts was discussed in *Abdul Ahad v. The State;* [608]

> "The most essential requirement of the law is that an expert on the particular subject whether Science, Art or Law including Muhammadan Law must be a master in the relevant field because of special duty, training, experience and extensive research work carried out. The opinion of such an expert alone would be relevant and admissible."

6.2.8.1 DNA and Scientific Evidence in Pakistani cases

Medical evidence like DNA, if proved to be genuine and corroborated, are irrefutable. Such evidence is one of the strongest proofs against the accused in cases of rape and other sexual crimes. There a large number of Pakistani cases shedding light on the issues of DNA.

---

[606] 2013 CL C 1171 [Peshawar]
[607] 1974 SCMR 311.
[608] PLD 2007 Peshawar 83.

6.2.8.2. Statutory framework

In Pakistan previously there was no particular legal framework which was addressing DNA proofs. In a very renowned judgment dealing with DNA evidence, *Salman Akram Raja & another v. Government of Punjab,* [609] it was observed by the court that DNA evidence is not conclusive on its own. It is considered valid if it is corroborated by other evidence.

In 2015, Honourable Supreme Court of Pakistan, in a kidnapping and murder case observed that DNA evidence was not admissible because there was no law regarding the admission of this type of evidence.[610]

This would have created confusion on the matter of admissibility of DNA evidence. Later on, the federal Legislator passed a law in 2016 "Criminal Law (Amendment) (Offences Relating to Rape) Act 2016". It amended section 164 of Criminal Procedure Code of Pakistan and added that samples of DNA, where practicable, shall be collected and sent for examination and scrutiny. [611]

Other than the current legislation on DNA evidence, it is also dealt with section 164 and section 59 of Qanun-e-Shahadat Order (QSO) 1984. Section 59 of QSO states that expert testimony on the matters of science and art is a 'relevant evidence'. While Section 64 stipulates, that evidence presented through modern means is admissible.

6.2.8.3. The Stance of Pakistan Courts on DNA Evidence

The purpose of explaining the stance of Pakistani courts on DNA evidence is aimed at exploring the present legal framework of Pakistan. There are two mainstream cases on the matter of DNA evidence. One of them is the matters pertaining to paternity. The other one is investigating sexual crimes.

---

[609] 2013 SCMR 203.

[610] Ali Chughtai, "Zainab's Murder: How will the Prosecution Build its Case?" Dawn, January 29, 2018, (lase accessed: July 6, 2018) https://www.dawn.com/news/1386000

[611] The Criminal Law (Amendments) (Offences Related to Rape) Act 2016 § 11.

1. Paternity Matters

Prophet PBUH has given us a golden principle to ascertain the paternity of a child, "a child is attributed to a person in whose wedlock he/she is born. [612] Pakistani legislature has tried to follow this rule by enacting Article 128 in QSO, which states that a child born after 6 lunar months of marriage and till two years of marriage shall be considered as the child of the person in whose wedlock he or she is born.[613]

A number of Pakistani cases elaborate on this principle. For instance, *Muhammad Arshad v Sughran Bibi,* [614] *in which suit of recovery of maintenance was filed by a mother and her minor child. Petitioner (father) disowned the child and refused to pay maintenance. Father gave an application for conducting a DNA test, which was refused. The court observed that DNA determination causes far-reaching consequences. Court added further that the claim for DNA test by father must be substantiated through other tangible proofs and credible evidence, which are absent from the petitioner's case.*

Another case *Sharafat Ali Ashraf v Additional District Judge, Bahawalpur,* [615] in which the petitioner refused any marriage, after a suit of maintenance was filed against him. A daughter was born while the case was still in progress. The family court decided that he is liable to pay maintenance to wife and child. Appellant court upheld the decision. The petitioner contended before the Supreme Court that he was subjected to gross injustice and that the DNA test must be conducted. Supreme Court observed that there were sufficient proofs of his marriage and that the decision of the lower courts was right.

In *Khizar Hayat v Additional District Judge, Kabirwala,*[616]maintenance was approved by the subordinate courts. The petitioner refused to be the father of a child. Eleven years after his birth, he

[612] *Hamida Begum v Murad Begum* PLD 1975 SC 624.
[613] Qanune-e-Shahadat Order 1984. Article 128.
[614] PLD 2008 Lahore 302.
[615] 2008 SCMR 1707.
[616] PLD 2010 Lahore 422

requested a DNA test. The court observed that DNA test cannot be ordered when it was already proven that the child was born during the wedlock and the petitioner has failed to bring any credible proofs of the illegitimacy of child.

It is worth mentioning that the Indian Supreme Court has adopted a different view on paternity matters. An Indian judgment explains very well the importance of DNA evidence in *Nandlal Wasudeo Badwaik v Lata Nandlal Badwaik & Anr*[617]

> "We may remember that Section 112 of the Evidence Act was enacted at a time when the modern scientific advancement and DNA test were not even in contemplation of the Legislature. The result of DNA test is said to be scientifically accurate. Although Section 112 raises a presumption of conclusive proof on satisfaction of the conditions enumerated therein but the same is rebuttable. The presumption may afford legitimate means of arriving at an affirmative legal conclusion. While the truth or fact is known, in our opinion, there is no need or room for any presumption. Where there is evidence to the contrary, the presumption is rebuttable and must yield to proof. Interest of justice is best served by ascertaining the truth and the court should be furnished with the best available science and may not be left to base upon presumptions, unless science has no answer to the facts in issue. In our opinion, when there is a conflict between a conclusive proof envisaged under law and a proof based on scientific advancement accepted by the world community to be correct, the latter must prevail over the former. "

The Supreme Court of Pakistan, on the other hand, has mainly being influenced by Article 128 of the QSO and a preference for the collective interest of society over an individual's interest in excluding DNA evidence, has been observed particularly, in paternity cases.

2. *Sexual Offences*

Another stream of cases in which Pakistani case law deal is sexual crimes. The approach adopted by the judiciary in this field is totally opposite to paternity matters. The difference of both lies may be due to the difference of legal framework pertaining to both the cases in QSO. DNA evidence has become prominent because science and technology have become advanced. Evidence which is available through modern means of science is admissible under Article 164 if Qanun-e-Shahadat.

[617] 2014 (5) CTC 680 <http://indiankanoon.org/doc/139951018/> accessed 15 November 2015.

The person who performs a DNA test bears an expert testimony; his statement is admissible under article 59 of QSO.[618]

The Mere presence of Article 164 is not enough for admissibility of DNA evidence. But there are certain criteria for acceptance. The legal framework has adversely impacted DNA in different ways. Considering this evidence as an expert testimony has reduced its potential to be treated as primary evidence. Expert testimony in Pakistan's legal framework is treated as corroboratory evidence and not primary evidence.

A very important judgment on matters related to DNA evidence was *Muhammad Shahid Sahil v The State,* [619] where the petitioner was accused of committing rape, in which the victim girl conceived and a baby girl was born. An application was made by the victim for conducting a DNA test, which was permitted by the judge. The accused/petitioner challenged the order for DNA test before the High Court. The latter did not find any legal infirmity in the order and confirmed it. The judge commented that once DNA test is complete, it will be produced in the court along with an expert opinion who conducted the test. The expert will be available for cross examination by the accused, who will have a sufficient opportunity to challenge the validity of such test. The court further opined that DNA test is the best possible evidence in the present case for unveiling the truth without any delay. The Judge expressed:

> "The prosecution agencies should take heed and use latest available technology to trace and locate the actual criminal. Under Article 164 of QSO, a court might allow being produced any evidence available because of modern devices or techniques. Furthermore, the Holy *Qur'an* and *Sunnah* did not forbid employing scientific or analytical methods in discovering the truth. On the contrary, the discovery and investigation had been strongly recommended by both. The courts in matters relating to Offence of Zina (Enforcement of Hudood) Ordinance 1979 had all the powers to permit reception of evidence including resort to DNA test, if demanded by the occasion. It is the fundamental duty of the courts to arrive at the truth without depriving an affected party to establish its point of view."

---

[618] Shehbaz Cheema, DNA Evidence in Pakistani Courts: An Analysis" *LUMS Law Journal* 3, 2016. (Last accessed: July 9, 2018) https://sahsol.lums.edu.pk/law-journal/dna-evidence-pakistani-courts-analysis#_ftnref23

[619] PLD 2010 FSC 215

The objection raised by the accused was rejected and he was ordered to appear for the DNA test of the three i.e. the accused, victim and the daughter.

Another very famous judgment on DNA test is *Salman Akram Raja v Government of Punjab*,[620] in which the apex court of Pakistan tried to fill the gap in legal framework for using DNA test in courts. The court directed that this test should be performed in all sexual offences and the samples of the test should be preserved also. The case was about a raped girl who later on committed suicide due to failure to get her complaint registered against powerful personals. Supreme Court took a suo moto action and addressed the issue. Observation of court regarding DNA test was "a mean[s] of identifying perpetrators with [a] high degree of confidence... [and] by using DNA technology the courts would be in a better position to reach at a conclusion whereby the real culprit would be convicted, potential suspects would be excluded and wrongfully involved accused would be exonerated."

The court advised that DNA evidence should not be admitted without corroboration of other proofs. The caution is correct as DNA evidence is not a conclusive proof and cannot be termed as infallible. As DNA evidence is "largely rooted in probabilities, even a confirmed "match" does not supply concrete proof of guilt". [621]

Supreme Court gave another principle of DNA testing. It was held that victim cannot be forced to give DNA test. On the contrary, accent of accused is not necessary. Because it is huge factor of ascertaining the truth.

A case *Mummad Ameen v The State*, [622] the High Court denied rejected the bail application even when the DNA report was not positive. The opinion of the court was based on the view that DNA test is just a secondary evidence and not primary evidence. The petitioner was an *imam* of a mosque, who was accused to have raped a student. The application of complaint was filed by the

---

[620] 2013 SCMR 203.

[621] Karen Norrgard, "Forensics, DNA fingerprinting, and CODIS." *Nature Education* 1, no. 1 (2008): 35. (Last Accessed July 10, 2018) https://www.nature.com/scitable/topicpage/forensics-dna-fingerprinting-and-codis-736

[622] 2013 PCrLJ 733 (Lahore).

girl's father. The court opined that no father would risk stigmatizing his daughter by falsely implicating someone.

The secondary status of DNA test has unfolded other aspects as well. If the case has been proved even without DNA evidence it is allowed. Like, if the facts of the case have been proved beyond reasonable doubt, such matter can be decided by court without DNA evidence.[623]

The judgments discussed above prove that DNA test is admissible in sexual crimes. But the evidential strength varies with the nature of the case. It is mostly dealt as corroboratory evidence, which cannot be conclusive evidence without other evidence. Even with some absolute and credible status of DNA test, it can be regarded as primary evidence. The problem which need to be addressed by the judiciary is to address the questions of in what circumstances should DNA evidence be collected? In what manner it can be used in offences and what should be its evidentiary value.

6.3 Cyber laws of Pakistan

A number of cyber laws are there in Pakistan which deal with electronic evidence. But primarily, there are three main laws dealing with electronic evidence in Pakistan. They are;

1. Electronic Transaction Ordinance (ETO) 2002
2. Qanūn-e-Shahādat Order (1964)
3. Prevention of cyber-crimes (PECA) 2016

6.3.1 Electronic Transaction Ordinance 2002 (ETO)

[623] Shehbaz Cheema, DNA Evidence in Pakistani Courts: An Analysis" *LUMS Law Journal* 3, 2016. (Last accessed: July 9, 2018) https://sahsol.lums.edu.pk/law-journal/dna-evidence-pakistani-courts-analysis#_ftnref23

In Pakistan, the Electronic Transaction Ordinance was enacted on September 11, 2002. ETO 2002 was promulgated after the challenging situation, which was created by the increased use of internet and e-commerce. This law was basically framed to give recognition to electronic transactions, electronically stored information and electronic evidence. On perusal of the preamble of Electronic Transaction Ordinance 2002, it is clear that this law was not enacted with the intention to penalize the offenders. The main objective of this law was to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers.[624] ETO resulted in certain amendments in Qanūn-e-Shahādat Order of Pakistan (described in the following section).

The Act has 39 sections and 9 chapters. Among these chapters the main chapters are recognition and presumption, electronic documents, certification service providers, certification council, and amendment in certain laws and offences.

The ETO 2002 considers electronic documents on the same standing as a physical document by giving legal recognition to electronic forms. Any document, record or information which is given in electronic form shall not be rejected on the ground that it is not attested by a witness[625]. Secondly, if any document is given in the court in electronic form it will be not be rejected on the ground that it is in electronic form. It means that the condition of writing does not exist in electronic form if it is usable and accessible for subsequent reference[626]. Similarly, ETO abolishes the condition of presenting the document in original if it is submitted in electronic form. This is subjected to the condition that there is assurance that the document extracted was authentic at the time when it was first generated.[627]

---

[624] Preamble of ETO. http://www.pakistanlaw.com/eto.pdf
[625] Pakistan Electronic Transaction Ordinance, 2002 § 3.
[626] Electronic Transaction Ordinance, 2002 § 3.
[627] Electronic Transaction Ordinance, 2002 § 5 clause (a) sub section 1.

6.3.1.1 Electronic Signature

Whenever documentary evidence is discussed, signature is the essential characteristic in order to testify about the authenticity of that particular document. Technology has innovated a solution to this problem in electronic documents, which is electronic signatures.

Subsection 1 (n) of Section 2 of Electronic Transaction Ordinance defines electronic signature as, "Electronic signature means any letters, numbers, symbols, images, characters or any combination thereof in electronic form, applied to, incorporated in or associated with an electronic document, with the intention of authenticating or approving the same, in order to establish authenticity or integrity, or both".

This definition tells us that e- signatures is a series of letters, alphabets or characteristics which are associated with an electronic document. It is further stated above that these signatures are used for authentication or establishment of integrity of document and that is it. This definition gives an impression that e-signatures are something very similar to passwords and security codes which are assigned to an email, a computer or a mobile phone. It will not be inappropriate to say that this definition is highly non-technical. Or it is so plainly defined that it may cause confusions for the legal advisors and judges to understand the true picture of e-signature. It might have been fine for 2002, when the ordinance was approved, but it must be updated and redefined for 2018.

Similarly, there is another definition given in E.T.O called as advanced electronic signatures[628], which says;

> "Advanced electronic signature" means an electronic signature which is either
> (i) Unique to the person signing it, capable of identifying such person, created in a manner or using a means under the sole control of the person using it, and attached to the electronic document to which it relates in a manner that any subsequent change in the electronic document is detectable; or
> (ii) Provided by an accredited certification service provider and accredited by the Certification Council as being capable of establishing authenticity and integrity of an electronic document".

[628] Ibid § 2, Sub section (1) clause (e).

This definition provides the concept of advanced electronic signatures. These signatures are different from the ordinary electronic signatures because they are specially accredited from the certification council.[629] This definition mentions that these signatures are under the control of the person who created it and that any changes made in future are detectable. But this definition does not define any method through which all this will be possible. The acceptable procedure and the criteria of admissibility remain undefined.

Both the definitions above seem incomplete. Studying the legal systems of other countries to see how they have explained and legislated on electronic signature, it is found that they have adopted effective and elaborative definitions of electronic signature laws. Definitions mentioned in the E.T.O lack explanation of the procedure and method of e-signatures. The types of e-signatures are not mentioned here. The definitions should insert certain explanations about the subject matter.

Section 7 of E.T.O deals with the legal recognition of "electronic signatures". Section 8 deals with electronic signature; "electronic signatures shall be approved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both".

This section states about electronic signatures, that it can be proved in any manner. It must identify some course of action so that any illegal method of proving e-signature can be curtailed. The laws should be vetted in such a way that they should show the clear intention of the law makers to the judges, lawyers and the public as well. In these three sections of ETO, it is difficult for the judges to get a clear picture of the idea of electronic signatures.[630] The definition is obsolete. There are no methods mentioned for authentication of electronic signatures. This Act was enacted with the intention of giving legal recognition to e-signatures. While the procedural details are totally

---

[629] This is the institution in Pakistan who gives the keys of e-signatures and certify them. This council was first time introduced in ETO 2002.

[630] Laws of other countries like India, Australia and Canada etc are very explained on this issue. This issue is very important now a days that is why majority of countries of world have legislated on electronic signatures. The laws of countries serve to be complete guide line for the public and jurors. For more details see http://electronicsignature.com/electronic-signature-laws-around-the-world/ (Accessed: January 15, 2017)

missing from ETO. For instance, India has very concisely and briefly elaborated the complete procedure of e-signature. Law of Canada[631] is also another good example to study.

6.3.1.2 Research Study: Law of India

Section 3 of the Indian Information Technology Act deals with digital signature in the following manner;

II. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE (AMENDED VIDE IT Act

> "(1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.
>
> (2) The authentication of the electronic record shall be affected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. Explanation.-For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-
>
> (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
>
> (b) that two electronic records can produce the same hash result using the algorithm.
>
> (3) Any person by the use of a public key of the subscriber can verify the electronic record.
>
> (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair."

The purpose of mentioning one section of Indian Information Technology Act 2000, is to create a ground for comparison for law in India and Pakistan. It can be analysed from above mentioned law that India's Law on authentication and other ways are so elaborative and explanatory. Pakistan on the other hand has not stepped out from mere permissibility of electronic evidence in court. In this modern age the strategy of legislatures should not be limited to "admissibility" but it should be a technical friendly approach and must give the answer to how? are much more elaborative than

[631] See Secure Electronic Signature Regulations (SOR/2005-30) it completely explains the technology process. authentication and all the other necessary details of electronic signatures. Available at: http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/index.html (Accessed February 15. 2017)

section 7, 8 and 9 of ETO 2002. This is just one example. IT Act is also much more elaborative on the issues related to cyber laws.

6.3.2.1 Electronically Generated Records

The term admission is broadened to compensate the electronically generated information as well. QSO states about the admissibility of electronically generated records as follows;

"46-A. Relevance of information generated, received or recorded by Automated system. — Statements in the form of electronic documents generated, received or recorded by an automated information system while it is in working order, are the relevant facts."[632]

Pakistan's law also recognizes computer generated records as admissible evidence. There is a necessary condition that the automated information system should be in working order at the time the record was created. [633]

There was a case, *Habib Metropolitan Bank Ltd. V. Mian Abdul Jabbar Gihllin*[634], which specifically talked about the admissibility of "computer generated records as admissible evidence" in which the court observed that;

".... For the defendants that the statement of the accounts filed by the plaintiff are not in accordance with law as the same do not bear the signature of the bank official and the stamp of the bank. The electronic Transaction Ordinance 2002 (ETO 2002) was promulgated with the view to provide recognition and facilitation of documents, records, information, communication and transactions in electronic form etc. By virtue of this Ordinance a legal cover has been provided to the electronic forms by categorizing that their legal recognition and admissibility etc. would not be called in question if the same has not been attested by any witness, in Case the same is in the electronic form. It is observed that rapid changes have occurred in the recent years as an older and conventional system of banking has been done away with to a great extent. In spite of having conventional and the old method banking system

---

[632] QSO 1964, § 46 Inserted By ETO 2002.
[633] The perspective of English law in detail on computer generated business records under the topics "2.2.2. Computer Generated records and 2.2.5.1. Business records".
[634] 2013 PLD 104 Karachi-High-Court-Sindh

latest technology has taken-over by way of introduction of electronic and digital methods. It is seen that the defendant has not denied obtaining of credit facility, but has only called into question the statement of accounts prepared electronically by submitting that this statement neither hears signature of bank official nor bank seal. Whereas these statements of accounts clearly stipulate that these are electronically generated documents and do not require any signature. Hence, in my view, these statements of accounts through which complete picture of the credit facility obtained by the defendant is quite visible would not be considered to be document having no legal authenticity. An examination of this statement of account show that they contain complete transaction with detail of accounts of the defendant and the same has duly been certified by the bankers."

It was observed in the case *Metropolitan steel corporation ltd. v. Mac steel international U.K Ltd.*[635] that;

"The learned counsel of the plaintiff has also argued that the sales contract has not been signed and therefore is not enforceable. As discussed above, the defendant has established that the sales contract was electronically sent to the plaintiff who acted on the same and opened a letter of credit in accordance with its term and conditions, which also contained an arbitration clause. The submission of the learned Advocate for the Plaintiff has no force in view of the provisions of the electronic Transaction Ordinance, 2002 .... In view of the aforesaid provisions of the electronic transaction ordinance, 2002, as well as amendment in the Qanūn-e-Shahādat Order, it appears that it is no longer necessary for electronically transmitted documents, which include commercial banking contracts, to be manually signed or for the same to be attested by any witness".

6.3.1.4 Analysis

Electronic Transaction Ordinance 2002, is a law which is very basic and general in nature and deals with a few issues very generally. This creates room for ambiguities and uncertainties. This law is not appropriate for the requirements of 2018.

Countries worldwide amend their laws regularly according to their updated requirements. The judiciary help legislatures to highlight any lacuna in laws. For instance, legislatures of USA amended the provisions on civil discovery, from Federal rules of Civil Procedure after a famous

[635] 2006 PLD 664 Karachi-High-Court-Sindh

case of *Zubulake.* [636] Later on, the law was amended after the court highlighted the lacuna in the law.

Similarly, India also amends their Information Technology Act when the Supreme Court of India highlights any lacuna or problem in the existing law.[637] The latest judgments of Supreme Court in India are full of knowledge and awareness for the lawyers and judges of lower courts to tackle the issues. On the other hand, Pakistan established their cyber courts in the year 2016. Before that the judges and the lawyers were not aware of the technical knowledge involved in the case. Thus, the lawyers could easily misguide the judges.

Recently, Indian Supreme Court has struck down Section 66 (A) of Information Technology Act which was curbing the fundamental right of "Freedom of expression". Adding further to the reasons of striking down the provision, the Court said that the words such as "annoying", "inconvenient" and "grossly offensive", used in the law are vague and not easy for the law enforcement agency to understand the nature and ingredient of the offence.[638]

Other provisions in Indian Information Technology Act 2000 also show the concern of the legislatures to frame flawless laws. Such as, the provisions on electronic signature quoted above is elaborative in nature with reference to the technicalities involved in it.

The legislations relevant to electronic signatures in ETO 2002, are suffering from two main issues. Firstly, considering the changing nature of electronic signatures, the law is obsolete. Secondly, the approach is non-regulatory.

---

[636] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003).

[637] There are a number of amendments on Information Technology Act 2000 on their website of Information Technology according to their needs. See Ministry of Electronics and Information Technology, Government of India.
http://meity.gov.in/content/information-technology-act

[638] Landmark judgment by SC; strikes down Section 66 (A) of IT Act, http://www.dnaindia.com/india/report-landmark-judgement-by-sc-strikes-down-section-66a-of-it-act-2071523

This is a fact that 'e-commerce legislation' is changing to non-regulatory approach as e-commerce is receiving a high rate of popularity. The laws should be elaborative enough to guide the lawyers and public. It should be able to literate or aware the judges and lawyers in the very least. In order to manage and tackle the changing demands of e-commerce, Pakistan needs to update its legal system as well. [639]

ETO is a local law and it is inadequate to cater the requirements of e-commerce, which is a global phenomenon. This law is conservative in nature. For instance, it does not deal with the issue of foreign Certifying Agents (CAs). In other words, it remains unclear whether certificates issued by foreign CAs are recognized in Pakistan. If such certificates are not recognized then the cross-border e-commerce will become unnecessarily limited in scope. An implicit assumption under the Electronic Transaction Ordinance on regulation of certification service providers and digital certificates issued by them appears to be that most of the electronic transactions undertaken on the internet are of the 'high-value' type. In other words, the value of the electronic transactions is high compared to the cost and money by obtaining a certificate from the CAs. This may be true in the case of 'business-to-business' e-commerce, but is not necessarily so in retail transactions. For example, electronic transactions of some goods, such as books, may not justify the cost of a certificate.[640]

Overall, ETO was a good effort as it was a timely legislation back in 2002, following the United Nations resolution recommending all members to adopt the Model law on Electronic Commerce adopted by the UNCITRAL. The Electronic Transactions Ordinance, deals with the recognition of e-documents, dispatch and receiving of e-documents, CSPs and Certification Councils. But it did

---

[639] Ibid 13

[640] Taymor Ali, "Legal environment of e-commerce in Pakistan", *Supreme Court of Pakistan* 12. (accessed June 12, 2017) supremecourt.gov.pk/ijc/Articles/10/3.pdf

not deal with the criminal matters such as data security concerns, breach of computer database theft, privacy violation. [641]

ETO 2002 also made some amendments in Qanūn-e-Shahādat Order 1984. These amendments along with the relevant judgments are discussed in the upcoming sections.

6.3.2 Qanūn-e-Shahādat Order (QSO)

Qanūn-e-Shahādat Order has been amended by the ETO to introduce the admissibility of electronic records. The concept of e-evidence has been incorporated to make the court available with a framework related to the modern advancements in the field of information technology.

QOS recognises electronic and automated data as a "document". It is stated that;

"(e) the expression, "automated", "electronic", "information", "information system", "electronic document", "electronic signature", "advanced electronic signature" and "security procedure", shall bear the meanings given in the Electronic Transactions Ordinance, 2002".

In accordance with the latest advancement in technology, the term "admission" is amended in article 30 of Qanoon-e-Shahadat Order as;

"Admission Defined: An admission is a statement, oral or documentary which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons and under the circumstances, hereinafter mentioned. [:]
1 [Explanation- Statements generated by an automated information system may be attributed to the person exercising power or control over the said information system.]"

As can be seen from the above cases, the QSO is not exhaustive. It does not provide the complete code for evidence. So it is possible to refer to judgments of foreign countries as persuasive laws.

[641] For these issues currently Prevention of Cyber-crimes Act 2016 is applicable in Pakistan. It is discussed later in this chapter.

The courts can look into the English common law or Indian cases, in case of doubt or ambiguity over the interpretation of any of the provisions of the QSO.[642]

An explanation of admissible evidence added in Article 73 of QSO by Electronic Transaction Ordinance is as follows;

"Explanation 3.—A printout or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form if the automated information system was in working order at all material times and, for the purposes thereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material times".

"Explanation 4.—A printout or other form of reproduction of an Electronic Document, other than a Document mentioned in Explanation 3 above, first generated, sent, received or stored in electronic form, shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored."

These two explanations of Qanūn-e-Shahādat Order 1964, article 73, inserted by Electronic Transaction Ordinance 2002, state that printout taken from automated information system shall be admissible and will be considered as primary evidence. And it does not matter if the printouts have many copies. All those copies shall be primary. These explanations have changed the concept of primary evidence. Majority of the legal systems of different countries have done the same. Previously, it was considered that primary evidence is the original and it must be presented in the court. But the documents which are generated from automated information system are considered primary evidence irrespective of their number of copies.

In another case, *Alamgir Chugtai v State*[643], the Lahore High Court of Pakistan discusses the same issue as follows;

"Similarly, extensive changes have been brought by the legislature in Qanūn-e-Shahādat, 1984 through second schedule of E.T.O.2002 to meet with the situation like present one and electronically gathered evidence is to be treated as primary evidence., So the documents tendered in evidence.... are admissible and duly proved and there is nothing on record which could show that narration therein was altered. I may observe here there is a case of cybercrime

[642] For instance, in case of Sikandar Ali Lashari v. State 2016 YLE 62 Karachi-High-court-Sindh the judge referred to a number of Indian as well as Western judgments. And he also cited law books of English writers on electronic evidence.

[643] 2009 PLD 254 Lahore-High-Court-Lahore

wherein latest technology was used whereby the whole operational system of the state was by-passed meaning thereby an advance and most revenue generating department of the state was set at naught with illegal installations. Such crime has become rampant in the society and that is the reason legislature in its wisdom has provided different a criterion about admissibility of evidence in such like cases. Now a days without any wire one can have the facility of connection all over the world and the whole business of the world is going on through Internet E-mail etc. and due to development in Science and Technology, it would not be possible to bring on record the physical existence of everything, as the whole technology is based on satellite operational networks."

In explanation 3 of article 73 of QSO stated above, the phrase "information system was in working order at all material" used is vague and controversial. It is an essential condition in Qanūn-e-Shahādat for the presumption of authentic data that the system on which that particular data resides must be reliable. But the words used for this purpose in law are that the: "security procedure was in working order at all material times". These words give birth to ambiguities while discussion during the trial. The security procedure for generation of secured electronic data is applicable when the document is generated. This document shall be received and saved by the recipient. The mentioned security procedure would probably suggest to be used at this end for verification. The problem is generally raised by the sender on the data integrity or the authentication process. The recipient, therefore, would probably not be in a condition to verify the working order of the information system at the time of record generation. Hence, the presumption should only require that the security procedure when applied in the presence of the court confirms the originator to be the alleged person. It is simply not easy to verify that the information system of the sender or receiver was in working order.[644]

6.3.3 Prevention of Cyber-Crime

As already discussed, Electronic Transaction Ordinance 2002, was a basic law and there were a number of deficiencies in it. It did not cover complete contents as per the requirements of modern

[644] Taymoor Ali, Legal environment of e-commerce in Pakistan ,13

technology of Pakistan. Electronic Transaction Ordinance 2002, was not legislated to penalize the offenders rather it recognizes the evidence derived from the modern techniques. Due to the increase in the use of computer, new ways of crimes have emerged. However, none of the new ways were included in this Ordinance. This made the legislation less effective. The effect of the legislation was that most offenders easily escaped from the law and judges were unable to frame charges against them.

Initially due to lack of any proper specific legislation on this subject, offenses relating to cybercrime were dealt under, Section 36 and 37 of Electronic Transaction Ordinance 2002. ETO was promulgated after accepting the challenging situation created by the increased use of internet and electronic commerce. Section 36 of ETO 2002 penalized the violation of privacy with imprisonment up to seven years, whereas Section 37 penalizes the damage to information system with imprisonment up to seven years.[645]

But it was not enough and there was a need of a law which could deal comprehensively with the issue of cyber law. That is why another law was enforced which was under preparation since 2004 onwards. That law was specifically meant to penalize the cyber-criminal and make the use of internet and e-commerce more secure.

6.3.3.1 Prevention of Electronic Crimes Ordinance of 2007

Keeping in view the deficiencies in ETO, another detailed law was introduced in the form of Ordinance, titled "Prevention of Electronic Crimes Ordinance 2007 (PECO 2007)". The scope of this ordinance was to cater the problems arising from misuse of technology. This Ordinance was legislated against cyber and electronic crimes. It penalized the criminal through effective legislation. Unfortunately, this ordinance law could not sustain because it was unable to attain the

[645]Noor Alam Khan, "Cyber Law", *Pakistan Journal*. No 43 (2014) http://www.pljlawsite.com/2014art43.htm (accessed January 30, 2018)

status of an Act, thus it lapsed in 2009. After that, offences relevant to cybercrimes were penalized under the ETO, once again. [646]

6.3.3.2 Prevention of Electronic Crimes Ordinance of 2009

When PECO 2007 lapsed after receiving three extensions, another law was passed in July 2009 by the President Asif Ali Zardari.[647] This ordinance was titled as the Prevention of Electronic Crimes Ordinance of 2009 ("PECO 2009"). It was similar to PECO 2007 and thus raised the same issues.[648] It lapsed in November 2009 for failure to secure parliamentary approval. Pakistan thereafter had no law to effectively prosecute cyber-crimes.[649]

6.3.3.3 *Prevention of Electronic Crimes (PECA 2016)*

From 2009 to 2016, Pakistan survived without any law that specifically deals with cybercrimes. The law enforcement agencies were dealing with the cases of cyber-crime under ETO as an alternative. There were a number of problems in courts in cyber-crime cases due to ETO, because it lacked penal provisions. [650]

---

[646] Ibid.

[647] Edidtor, Placing Lapsed Ordinance in Senate: Law Ministry Apologises to Committee, *Dawn*, (June 23, 2010), http://www.dawn.com/news/850187/placing-lapsed-ordinance-in-senate-law-ministry-apologises-to-committee. The ordinances were first passed in December 2007, and then re-promulgated in May 2008, February 2009 and July 2009. *See* Fazal Sher, *Prevention of Electronic Crimes Bill: NA Body Seeks Recommendations*, Business Recorder, (June 30, 2012), http://www.brecorder.com/top-news/108/64900-prevention-of-electronic-crimes-bill-na-body-seeks-recommendations-.html.

[648] Mohammed, Furqan, PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill, Journal of Islamic and Near Eastern Law, 15(1) 2016. 74. (Accessed March 17, 2017) http://escholarship.org/uc/item/14x2s9nr.

[649] Azam Khan, *NA Session on Cybercrime Bill 2015 Postponed Till Next Week*, The Express Tribune, (Apr. 24, 2015), http://tribune.com.pk/story/875246/na-session-on-cybercrime-bill-2015-postponed-till-next-week/ (noting that both PECO 2007 and PECO 2009 had failed to secure parliamentary approval). After the lapse, the government went back to utilizing the Electronic Transactions Ordinance of 2002 ("ETO 2002") to prosecute crimes. *See* Jahanzaib Haque, *Open Democratic Initiative: Developing a Progressive Internet Policy for Pakistan*, Jinnah Inst. Policy Brief, (Jan. 30, 2015), http://jinnah-institute.org/wp-content/uploads/2015/01/Internet-Policy-Brief.pdf. The ETO 2002 was the first IT-relevant legislation passed by Pakistan.

[650] Omair Zeeshan, *Investigators Suffering from Absence of Law*, The Express Tribune, (Mar. 24, 2011), http://tribune.com.pk/story/ 136794/investigators-suffering-from-absence-of-law/.

The people of Pakistan, particularly IT industry was suffering in the absence of adequate cybercrime legislation. In the absence of relevant law, cyber criminals were operating without any fear or accountability. Furthermore, due to the absence of an intermediary liability protection clauses, many big IT companies were reluctant to make investments in Pakistan.[651]

After passing of six years, fortunately, cybercrime laws came under limelight again in 2014 when the bill was introduced before Parliament. The bill, namely Prevention of Electronic Crimes Bill 2014 was introduced and presented before the National Assembly. There was a heated debate on the Act. But finally, this bill got the approval after two years and was approved in 2016, attaining the status of an Act. The Prevention of Electronic Crimes Act gained a lot of popularity among the society and it received a lot of discussion, debates and both positive and negative criticism. The reason behind the mixed reviews was that it covered a large number of crimes in it. In this act, punishments related to unauthorized access, copying, transmission, interference with information system and critical infrastructure information system or data are discussed. [652]

In the situation when Pakistan had not a single law dealing with cyber-crimes, it was a great fortune that the law was passed. It was a need of the public as there were cases of social media harassment. The financial institutions also needed a law as they faced gross level stealing of money through cyber-crimes.

6.3.3.3.1 List of Offenses and Punishments

A number of cyber-crimes and their punishments are mentioned in PECA 2016, which includes spreading false information about someone. Its punishment is 3 years imprisonment and 1 million rupees fine or both. Spreading or making of explicit videos of an Individual can be punished up to 5 years or up to 5 million fine or both. Doing the same in case of a minor has results in punishment of

[651] Saghir Anwar, Cyber Crime bill: Misconceptions and realities, The News April 25, 2015. (Accessed March 17, 2017) https://www.thenews.com.pk/print/37082-cindy-sheehan-arrested-for-protesting-outside-bush%E2%80%99s-ranch

[652] Ibid

7 years prison or 5 million fine. Someone who intentionally produces, distributes or transmit material related to child pornography will have 7 years punishment or 5 Million fine or both. Punishment of Cyber stalking is up to 3 years in jail or 1 million fine or both. Hacking of an email or stalking will cause jail up to 3 years or 1 million fine or both. Punishment of making videos/ pictures and distribution without consent is up to 3 years jail or 1 million fine or both. Hate speech is also a crime and its punishment is up to 7 years in prison or fine or both. Punishment of spamming is 3 months of imprisonment or fine up to Rs. 5 million or both. etc

6.3.3.3.2 Analysis

This bill was highly opposed by the Human Rights Foundations and NGO's but despite of severe criticism, it is now part of the law of Pakistan. The main reasons for criticism made by the NGO's was that this law is draconian.[653] It curbs Human Rights and by giving overreaching powers to Law Enforcement Agencies[654]

Following were the main points on which this law was criticized;

8. The drafting and definitions are broad, vague and can be interpreted in many ways.
9. There are some serious issues regarding the privacy of citizens and curbs fundamental rights of citizenship.
10. This law gives sweeping powers to the law enforcement agencies to block any source of information.

[653] Raza Khan, "Controversial Cyber Crime Bill approved by NA" Dawn, April 13, 2017. Accessed February 28, 2010.
https://www.dawn.com/news/1251853
[654] Ibid.

11. This is a draconian law.[655]

The first criticism, as already stated that this law is loosely drafted[656] and it is very broad in scope and can be interpreted in many ways. Few illustrations below will support the argument:

For instance, in "act" is defined in Sec 2 (a) (i) of PECA as "series of acts or omissions contrary to the provisions of this Act". This word is very confusing as the word 'act' is undefined in the definition.

Similarly, "access to data" is defined in Sec 2 (b) as gaining control or ability to read, use, copy, modify or delete any data held in or generated by any device or information system. This is also a very broad definition for control of data which has a potential for misuse. The meaning of the word "access to information" in section 2 (c) is "gaining control or ability to use any part or whole of an information system whether or not through infringing any security means". This definition similar to 'access to data', is very general in nature and does not convey to the actual meaning.[657]

Sec 2 (n) defines the word dishonest intention as "intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred;" this definition is criticized as being a statement which is very loosely drafted and that the term is very vague[658]

There is another definition of dishonesty in Pakistan Penal Code.[659] But that definition is precise with wrongful gain and loss. But here the word 'creates hatred' is a vague term and it can be

---

[655] Raza Khan, "Controversial Cyber Crime Bill approved by NA" Dawn, April 13, 2017. Accessed February 28, 2010.
https://www.dawn.com/news/1251853

[656] Ibid.

[657] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016" , 2. Accessed February 28, 2010. www.netfreedom.pk/wp-content/.../2016/.../CSO-criticism-on-PECB-2016_IssuePaper.pdf.

[658] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016" Bytes for all, Impact and Association for Progress communication, 3. Accessed March 1, 2017. www.netfreedom.pk/wp-content/.../2016/.../CSO-criticism-on-PECB-2016_IssuePaper.pdf

[659] Section 24 of Pakistan Penal Code defines as "Dishonestly: Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing dishonestly".

interpreted in many different ways, especially in the context of sectarian environment of Pakistan. The word "create hatred" should either be omitted or should be drafted in a precise manner.

The criticism was so intense that it even criticized some provisions which were not that problematic. Such as, the definition of word "critical infrastructure", highlighted as being loosely drafted[660], states that "Any other private or Government infrastructure designated by the Government as critical infrastructure as may be prescribed under this Act." It was stated that this word does not clearly define the critical infrastructure.

Although, these kinds of statutes are already present in Indian Information Technology Act 2000 since 2008[661], these issues are not criticized as in Pakistan. [662]

Section 9 of PECA was also badly criticized for using broad wordings and for curbing freedom of expression. Large number of NGO's in Pakistan were at the stance that if implemented it will suppress any type of debate on issues of public interest including national security, terrorism or about an accused or convicted of crimes [663] This section is also considered as a serious threat to the ability of journalists to work freely.[664]

---

[660] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016" Bytes for all, Reporters Without Borders (RWB) and freedom network, "Analysis of Pakistan's cybercrime Bill" Accessed March 1, 2017. https://rsf.org/sites/default/files/analysis_of_pakistan_s_cyber-crime_bill.pdf (Reporters without Border is a France based non-profit organization that promotes freedom of information and freedom of press).

[661] Section 70 A sub clause 1 of Indian Information Technology states that "The Central Government may, by notification published in the official Gazette, designate any organization of the Government as the national nodal agency in respect of Critical Information Infrastructure Protection". Accessed March 1, 2017. http://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf

[662] Here even the positive things are criticized so much for political purposes that they take a lot of time in approval e.g., CPEC.

[663] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016" Bytes for all, Impact and Association for Progress communication, 4.

[664] Reporters without Borders (RWB) and freedom network, "Analysis of Pakistan's cybercrime Bill", 3.

Section 9 of PECA states: "-(l) Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

Explanation -For the purposes of this section "glorification" includes depiction of any form of praise or celebration in a desirable manner."

"Glorification of offences related to terrorism" is an area which needs serious attention from the state. Legislating on such sensitive issues should not be subjected to criticism. Threats of terrorism is widespread in Pakistan and is weakening the roots of the State. A dire need is there, to regulate it through law. Terrorists are using information technology as an essential tool. So, there should be laws to curb terrorism.

Other provisions of Sections 14[665], 15[666], 16[667], 17, 22, 23, 27, 28, 29, 30, 31, 32, 33, and 45 are objected for being drafted in a vague, ambiguous and broad manner. These provisions are said to be drafted loosely, leaving huge space for interpretation and provide for broad punitive measures. [668]

Thorough study of rulings prove that these sections can be narrowed down by judicial interpretations. But there must be some room for the courts to interpret, and discuss. Large number of other words are narrowed down by Pakistani courts, in other laws.

---

[665] It deals with Electronic fraud and says: "Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend lo two years or with fine which may extend to ten million rupees or with both"

[666] It is about making, obtaining or supplying device for use in offence

[667] Unauthorized use of identity information.

[668] Haroon Baloch, "Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016" Bytes for all, Impact and Association for Progress communication, 9.

The second major criticism of this law is that it curtails privacy of citizens. This law gives sweeping powers to the law enforcement Agencies to block or access any data. Section 37 of PECA 2016 says:

"The authority shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offense under this Act."

This section was subjected to heavy criticism, stating it to be against the fundamental rights of the citizens of Pakistan and granting such powers to the authorities is not legal. But PTA is enjoying these powers since 1998 under PTA Act.[669] Section 54 of Telecommunication Act 1996 allows the Government of Pakistan, to intercept and trace calls and messages, through its agents. This power is exercisable in "national security" and in "apprehension of offense".

Discretion and the power of Government of Pakistan is very broad. There is no check and balance system or direct recourse to judicial authority against such decisions and orders of Government of Pakistan. It presumably stays as a secret.

Fourth criticism of this law is that it is draconian. It gives punishments that are harsh in nature. But there are almost the same kind of punishments in Indian Information technology act 2000[670]. For instance, Section 66 E penalize with 3 years' imprisonment to those who intentionally publish

[669] Section 54 of Telecom Act 1996 reads: "Notwithstanding anything contained in any law for the time being in force, in the interest of national security or in the apprehension of any offence, the Federal Government may authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system."

[670] Punishments of imprisonment are same; the monetary punishments are higher in Pakistan though.

or transmit pictures of private areas of some person to destroy his reputation.[671] Same is the punishment for this offense in Pakistan under section 20 of PECA 2016.[672]

Pakistan was desperately in need of a law which could penalize cyber-criminals. It was decided and discussed at different forums at the time that in the present technological age, cyber space is the most effective warzone of the present times. So we need some very efficient laws to deal with day to day threats to cyber security.[673]

6.4 Issues in the legal system

As part of primary research, a visit was made to the National Response Centre for Cyber Crime (NR3C) Islamabad to interview Mr. Mehmood ul Hassan, a forensic expert of NE3C of FIA. Following are the enforcement issues which were reported by FIA during the interview:

1. All the offences except three are non-cognizable.
2. Judges are not well trained.
3. Courts are not well equipped.
4. There is no awareness among the masses.
5. Investigation Officers are very less in number.
6. International Liaison.
7. Capacity Building is a great problem.
8. Lack of infrastructure.

These following sections shall discuss the above eight issues in detail.

---

[671] Indian Information Technology Act 2000, Section 66 E
http://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf

[672] Sec 30 of PPC. Acessed: May 9, 2017)
http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj

[673] It is observed by different experts that "In order to battle cyber-crime…local security policies, cooperation with international security policy makers, e Crime laws, organisational cyber laws, privacy laws and data protection laws were the need of the hour." https://tribune.com.pk/story/769324/regulating-cyberspace-call-for-legislation-on-cyber-security/

6.4.1 Non-Cognizable Offences

A very serious issue being faced by the law enforcement agency regarding PECA is that, with the exception of three, all the offenses included in PECA are non- cognizable. [674] In Pakistan's legal system, procedures such as, taking permission from the court, giving application and pursuing the legal requirements to get the warrants, etc are time consuming processes. Under the current status of affairs, the following situation was likely to occur, there is a person caught by the bank authorities red handed inside the ATM. The bank calls FIA to arrest him, FIA cannot arrest him before getting approval from the court. Till the time the arrest approval is acquired, the offender probably has removed all the proof and evidence against himself.

The fragile nature of electronic evidence is known publicly. Electronic evidence can be wasted or tampered with in the shortest span of time. In present time, almost majority of the evidence is hidden in mobile phones, which include communications, messages, pictures, and sometimes notes. If the offense is non-cognizable, the Investigation authorities are required to give application in court. Then the court, if it thinks appropriate, will issue warrants. Only after issuance of warrant, the investigation officer can arrest the accused. During all this processing, the accused can break or destroy the medium in which evidence is present e.g. phone, laptop, hard drive, etc.

It is tried by FIA to apply section 420 PPC and arrest, but this is not the correct procedure for arresting. It is demanded by the officials of the FIA that offense should be made cognizable. It is practically impossible to go to court, take warrant and get the approval while the offender would be waiting for the investigation agencies with the evidence in hands, to be arrested. By that time the evidence is destroyed. And the case ceases to proceed without evidence.

---

[674] Section **43 of PECA states that Offences to be compoundable and non-cognizable.** — (1) All offences under this Act, except the offences under sections 10, 21 and 22 and abetment thereof, shall be non-cognizable, bail able and compoundable.

6.4.2 Untrained Judges

Another great problem highlighted during the interview was that there is a dire need of proper training of judges. Judges are not trained enough to understand the problems of electronic evidence. It is said that the lawyers misguide the judges on these modern terminologies about which the judges are usually not well aware.

6.4.3 Ill-Equipped Courts

The courts are not well-equipped for displaying and handling of electronic evidence. For instance, computers, multimedia to show and exhibit electronic evidence in court.

6.4.4 Limited Investigation Officers

The number of investigation officers is extremely low as compared to the number of complaints registered with NR3C. It was told by the officer that there is a massive response of public to the NR3C cell. For about 2500 complaints they had only four to five investigation officers. It is practically impossible for one investigation officer to deal with 500 cases at the same time.

6.4.5 International Liaison

A very essential treaty for cyber-crime called Convention on Cyber Crime (CCC) exists that allows the social media companies to share data with the countries part of the treaty. Pakistan is currently not part of CCC. If Pakistan signs this treaty then the management of Skype, Facebook, Google, Yahoo, etc. will be bound to recover the data demanded by Pakistan. Otherwise, if Pakistan requires any data regarding any cyber-crime and which they refuse to give, Pakistan cannot force them because it is not from their signatories.

6.4.6 Lack of Mass Awareness

Generally, there is no awareness in the public regarding the matters which are related to cyber-crimes. People do not know, where to go in case of they are subject to cyber-crimes. The

procedures and digital rights are not discussed. Secondly, the lawyers and judges are in the phase of learning how to deal with electronic evidence at court. The general public is much more below in this level.

6.4.7 Capacity Building

There is a strong need train people. As there is lack of trained IT professionals. There is only one department, dealing with complaints regarding cyber-crimes, i.e. NR3C. Each one of the investigation officers in NR3C, has to deal with 400-500 cyber-crime cases at the same time. This ratio is too high for one person.

6.4.8 Lack of Infrastructure

Lack of infrastructure is a serious problem. Space with latest technology and high-speed uninterrupted internet must be given to the professional dealing with cyber-crime complaints. The way manpower is less in Pakistan to deal with these cases, infrastructure is also not in a very good condition.

6.5 Conclusion

Pakistani law on Electronic Evidence is brief general and less elaborative. Mainly three laws deal with electronic evidence and its admissibility. The first one of them Electronic Transaction Ordinance 2002 (ETO). The legislations relevant to electronic signatures in ETO 2002, are suffering from two main issues. Firstly, considering the changing nature of electronic signatures, the law is obsolete. Secondly, the approach is non-regulatory.

ETO is a local law and it is inadequate to cater the requirements of e-commerce, which is a global phenomenon. This law is conservative in nature. For instance, it does not deal with the issue

of foreign Certifying Agents (CAs). In other words, it remains unclear whether certificates issued by foreign CAs are recognized in Pakistan.

Qanūn-e-Shahādat Order 1964(QSO), has been amended by the ETO to introduce the admissibility of electronic records. The concept of e-evidence has been incorporated to make the court available with a framework related to the modern advancements in the field of information technology. QSO clearly deals Computer Generated Evidence, Evidence from modern devices etc.

Both ETO and QSO does not deal comprehensively with electronic crimes. For that Prevention of Electronic Crimes Act 2016 (PECA) was legislated. It deals with all type of cyber-crimes.

In the situation when Pakistan had not a single law dealing with cyber-crimes, it was a great fortune that the law was passed. It was a need of the public as there were cases of social media harassment. The financial institutions also needed a law as they faced gross level stealing of money through cyber-crimes.

This bill was highly opposed by the Human Rights Foundations and NGO's but despite of severe criticism, it is now part of the law of Pakistan. The main reasons for criticism made by the NGO's was that this law is draconian. It curbs Human Rights and by giving overreaching powers to Law Enforcement Agencies.

CHAPTER 7

CONCLUSION

7.1 Conclusion

Electronic evidence is a very vast and fast-growing field whether it be the U.S law, Islamic law or Pakistani law. Developments in the law are being made on a daily basis. New principles are evolving which is creating more options for research and development.

This thesis primarily aimed at researching three main questions. The main focus of these three questions was to analyse the admissibility of electronic evidence in commercial transactions. Firstly, the evaluation of Sharī'ah Standards for electronic evidence. Secondly, the standing of U.S law on electronic evidence. And lastly, analysis of the Pakistani law with regards to electronic evidence. Comparative analysis of above mentioned three legal systems is aimed in this chapter, in order to propose some recommendations for Pakistani law.

Western law's view point on electronic evidence is that they pass it through four tests for admissibility. If the evidence passes these tests, it is admissible.

These are;

1. Relevance[675]
2. Authentication[676]
3. Hearsay[677]
4. Best evidence rule[678]

Besides the similarities with the Western Law, the Islamic law has different steps of proving or disproving facts. The means of proofs in the Islamic law are seven in total;

1. Oath [679]

[675] See above chapter 3, para 3.3
[676] See above chapter 3, para 3.4
[677] See above chapter 4, para 4.2
[678] See above chapter 4, para 4.3

2. Confession [680]
3. Oral testimony [681]
4. Documentary evidence [682]
5. Expert testimony [683]
6. Circumstantial Evidence [684]
7. Knowledge of the Judge.

These means of proofs are acceptable in the English law as well. For instance, Oral testimony is admissible in both the legal systems. Documentary evidence, expert evidence and circumstantial evidence are equally acceptable in the both and are treated as independent means of proof. As Islamic law came much earlier than the Western law, it can be easily stated that the Western law is derived from the Islamic law. And as both the Islamic law and the Western law are the same in terms of law of evidence, the same rules will be applied to electronic evidence as well. However, the major differences in Islamic law with regards to the permissibility of electronic evidence in Shari'ah perspective will be applicable.

The third legal system as already stated is Pakistan's. there are a number of statutes dealing with electronic evidence. For instance, National Accountability Ordinance 1999, Pakistan Telecommunication Act 1999, etc. But specifically, three laws are focused on cyber laws.

1. Electronic Transaction Ordinance 2002.
2. Qanun-e-Shahadat Order 1984.
3. Prevention of Electronic Crimes Act 2016

---

[679] See above chapter 2, para 2.3.1.
[680] See above chapter 2, para 2.3.2.
[681] See above chapter 2, para 2.3.3.
[682] See above chapter 2, para 2.3.4.
[683] See above chapter 2, para 2.3.5.
[684] See above chapter 2, para 2.3.6.

Focus of first two laws is basically on electronic commercial transactions. By way of these two doors of electronic commerce in Pakistan opened. All the provisions in both of them pertain to electronic contracts, electronic signatures, electronic data and others etc. This chapter will compare above mentioned means of proofs one after the other in all three legal systems.

Oral testimony is the first and the most important means of proof in both the Islamic and Western law, but with a lot of differences. For instance, Islamic law does not accept testimony of a person who is not just in character (Ādil). According to Islamic law, a testimony for electronic evidence must be taken by a just witness. A witness who has a doubtful character cannot lead to truth. There is a long discussion of Muslim jurists explaining the attributes of a just witness. [685] Although the standards of the Muslim Jurists regarding these characteristics relaxed with the passage of time, there is still a criterion to meet. [686] English law does not stipulate any such condition on witnesses.[687] In it generally a witness is capable of giving testimony. There are no such conditions stipulated in Qanun-e-S00hahadat Order as well, which is the prime law of evidence in Pakistan.

Islamic law also introduces a highly effective mechanism of purgation of witnesses.[688] It developed a complete system of accredited witnesses who subsequently became the helpers of the judge.[689] English law on the other hand does not expressly stipulates any methods of purgation in law of evidence as mentioned by Qura'an.

---

[685] See above chapter 2, para 2.3.3.9.
[686] The standards set by Imam Abū Ḥanīfa were bit stricter than his disciples. The reason given for this law was change in environment.
[687] English civil law discusses testimony of wife who cannot testify in case she is jointly liable with husband otherwise she can testify.
LexisNexis, Witnesses-Overview,
Available at:https://www.lexisnexis.com/uk/lexispsl/corporatecrime/document/391421/591F-WM31-F188-N326-00000-00/Witnesses_overview (Last accessed November 3, 2020)
[688] See above chapter 2, para 2.3.3.12.
[689] See above chapter 2, para 2.3.4.2.

The law of Pakistan on oral testimony is influenced by English Law because Qanun-e-Shahadat order 1984 was previously called Evidence Act 1872, which is an English law. QSO 1984 is a mere repetition of Evidence Ac 1872 except few articles, like article 3, 4 to 6 with reference to Hudood law, addition to art 44 and addition of a proviso to Art 42. The standard applied for oral testimony are those which are followed in western law.

In addition to this English law, U.S law and laws of developed countries are updated with respect to electronic evidence. Pakistani law on the other hand, lags behind as per international standards. There are a number of things, which need to be added in order to update it according to international standards. For instance, it does not discuss whether oral testimony is required for electronic evidence or not. What shall be the requirement of oral testimony?

So, the standards applied for oral testimony in QSO 1984, are those which are in English law. These standards have nothing to do with Islamic laws. Although Pakistan is a Muslim country but the laws being followed by them are western. Same is the case with electronic evidence. Witnesses who come for testimony for e-evidence are the ones which qualify through English law. The qualification for admissibility of oral testimony, in Pakistan, must be based on Sharī'ah.

Different classifications in terms of number of witnesses also adds in to the differences between Western and Islamic law. [690] The number of witness must be followed as prescribed in *Qur'an* for admission of electronic evidence. At least, four witnesses are necessary for testifying in case of Hudūd offences, such as slandering and fornication. Other crimes and financial matters require at least two witnesses. English law does not stipulate such

[690] See above chapter 2, para 2.3.3.6.

conditions. There is no classification such as *Ḥadd* offences and other offences. Pakistani law is completely silent on these matters, which means it follows English law.

Unlike English Law, the Islamic law differentiates in women testimony[691]. Women are not allowed to testify in cases of *Ḥudūd* and *Qisās*. It is proven by the *Sunnah* of Prophet (PBUH) and *'Ijma'*. It is allowed only in cases other than *Ḥudūd* and *Qiṣāṣ*, financial matters, property, marriage, divorce, freeing of slave, *'Iddah* and *sulḥ*, etc. Opinion of scholars is different regarding admissibility of women's testimony, which would be equally applicable to electronic evidence. [692]

There is a list of differences between male and female testimony. The biggest among them is she cannot testify in case of Hudūd and Qisās. Another one of them is that in case her testimony is admitted, two women would replace one male testimony.

English law does not differentiate between both testimonies. Same is the case with Pakistani law. As Pakistani law is following English evidence law.

Documentary evidence is the second most important means of proof in Islamic law. It not only permits documentary evidence but also accepts it as one of the strongest mean of proof. Allah the Almighty has commanded in *Qur'an*, to put in writing the contract taking place between the parties, to avoid conflicts and problems at a later stage.[693] Documentary evidence has prime importance in the realm of electronic evidence as well. The laws of different states and Qanūn-e-Shahādat Order consider e-evidence as documentary evidence. [694] Due to this reason there is a link between electronic evidence and Shari'ah.

---

[691] See above chapter 2, para 2.3.3.11.
[692] See above chapter 2, para 2.3.3.9.
[693] See above chapter 2, para 2.3.4.1.
[694] Qanun-e-Shahadat Order 1964, § 164,, See above chapter 2, para 6.4.2.

Admissibility of e-evidence in Islamic law is established but certain criterias must be fulfilled. These pre-requisites are provenance and chain of custody. Documentary evidence is admissible subject to oral testimony. It was a common practice to draw up such documents before *Qādi* and deposit them back in court's archives for safe keeping. [695] Documents saved in archives of court i.e. Maḥādir and Sijīlāt are also admissible. [696] *Mālikī* school of thought accepts documentary evidence after approval of two qualified witnesses. *Ḥanafi*s also accept written evidence as valid evidence if there are no possibilities of falsification of document and it has been preserved in the archives of the courts.

Admissibility of electronic evidence in the Islamic law is subject to credibility of the document as well. If the document is placed in a safe custody and is free from all the dangers of alteration and fabrication, it is admissible.

Documentary evidence is highly reliable in English as well as Pakistani law. It is approved world-wide that all the electronic evidence, such as CCTV video, SMS, emails, websites, ATM, records, call records etc. are documentary evidence and are admissible. Pakistani law also affirms in a number of judgements where they have considered USB, CDS, voice records videos etc., as documentary and admissible evidence. [697]

Third most important mean of proof for e-evidence both in Western and Islamic law is the expert witness. Experts include, cyber security experts who have mastery over mobile forensics, IT experts and investigation officers. They are required to be in court for technical cases which are beyond the knowledge of judges and lawyers.

---

[695] Ibid.
[696] See above chapter 2, para 2.3.4.2.
[697] See chap 6, para 6.2.7.

In the classical Islamic history, it was a matter of routine to seek the help of experts wherever it was required. It can be observed that the Prophet (PBUH) and the Righteous Caliphs either demonstrated expert quality or used expert witnesses wherever required. [698]

Scholars have debated on status of expert testimony. Sometimes they refer to it as *shahādah* (testimony) and sometimes as a report. This creates a confusion as to whether the jurists should consider expert testimony as a khabar when one witness is required or as a *shahādah* when two witnesses are required. If one witness is sufficient, the juristic justifications for relaxation of evidentiary requirements need to be known.

There is a difference of opinion among the scholars as to whether the expert testimony should be treated as a testimony or a report. There are a large number of examples quoted in classical Islamic Law.[699] Jurists have also differed in opinions regarding the requirement of number of witnesses in each matter such as, defects of slaves, evaluation of property.[700]

In the case of value of damages for movable and immovable property and rental prices etc., *Ibn Abidīn* requires testimony of two expert witnesses. *Sarakhsī* requires two expert witnesses too. He said if the expert differed in opinion regarding stolen property, if it is greater than or less than nisāb. The *ḥadd* punishment shall be prevented due to presence of *shubha*. *Imām Mālik* permits single testimony in property matters. In case of al *qāsim* (divider) *Imam Malik* says that one testimony is acceptable but two are better *(al-aḥsan)*. [701]

---

[698] For instance, when a woman wanted to slander an innocent man for committing her rape and she spilled egg white on her clothes and thighs. Caliph Ali boiled the egg white and tasted it. That is how he discovered the reality. Similarly, once two brothers came to the Prophet (PBUH) to resolve the issue of a disputed property among them. Prophet (PBUH) sent Hudhayfa b. al-Yaman (God be pleased with him) to decide the issue. He decided in the favour of the party whose property was adjacent to the knots that has been made in strings that supported the fence. When he told Prophet (PBUH) about it. He praised him for making such a decision.

[699] See above chapter 2, para 2.3.5.4.

[700] For defects of slaves, Imām Sarakhsi states two male testimonies are required.

[701] See above chapter 2, para 2.3.5.2.

Examination of the Islamic law clearly shows that sometimes jurists treat expert testimony as report and sometimes as witness and require number of experts explicitly mentioned in *Qur'an* and *Sunnah*. Sometimes Prophet (PBUH) relied on the opinion of one expert. [702]

The factor of necessity is also a very important element for demanding one witness. For compilation of Ḥadith, due to the fear of losing the binding dictums of Prophet (PBUH), one person's testimony was valid in matters related to rituals. Similarly, in matters related to rituals, due to fear of prejudicing God's right, one expert testimony was permissible because sometimes it was impossible to find two just and qualified expert witnesses in a case.[703] Mostly, jurists require two experts in majority of cases (including women's related matters) to increase the probability of witness. But they were ready to adjust with single testimony at the time of necessity (Darūralı).

The same rule is applicable to female testimony, the jurists who considered female testimony as report admitted one testimony, but for higher reliability they preferred to have two testimonies. Likewise, the scholars who considered it as a testimony require two but on grounds of necessity, they accept one.

Admissibility of Expert testimony in English law is different from Islamic law. The two main characteristics for expert testimony in the Western Law are;

1. Scientific dictums must be based on facts derived from experiments
2. Scientific laws and factual dictums must be quantified and mathematically presented

Since 1923, the role of experts in US legal system is based on Frye dictum. According to this rule, it is the role of the judge to check whether a scientific position presented before the court

---

[702] Like Zaid b. Thabit translated Jewish scriptures for Prophet (PBUH). Such cases encourage the jurists to make an opinion that expert testimony is just like a matter as transmission of Hadith. Which means one witness is enough.

[703] See above chapter 2. para 2.3.5.2.

is the accepted position of the relevant scientific community. In 1993, the Daubert precedent replaced the Fryer rule. This rule added four more criteria to the one prescribed by Frye. These are, testability, peer review, error rate, and standardization.[704]

Islamic law considered expert opinion as "testimony". That is why most of the jurists admitted testimony of two just witnesses, where two are not available, one is acceptable on the ground of necessity. Authentication techniques also applied to experts, like other because they are also treated as witnesses, not as a report (khabar).

So the modern approaches to expert testimony are also correct i.e. peer review, testability error rate and standardization. Because these somehow serve to be authentication techniques. Secondly, expert is called in court for cross examination is another part of authentication process.

Pakistani law admits oral testimony under Art 59 of QSO 1984. It says that expert testimony is admissible in order to check the integrity of an electronic document. It does not stipulate any conditions regarding the qualification of experts stated in English or Islamic law. There is no specification of particular number of expert witness, as stated in Islamic law. Pakistani judgements however mention that expert witness is corroboratory in nature and that the expert is open for cross examination in courts. There is still a need to upgrade the standards set for expert testimony in Pakistani law. [705]

Circumstantial evidence has always been a strong mean of proof in the eyes of both the Western law and the Islamic law. There are two types of circumstantial evidence in Islamic law:

4. Strong Circumstantial Evidence (*Qarīnah Qāti'ah)*

[704] See above chapter 2, para 2.3.5.2.
[705] See chap 6, para 6.2.8.

5. Weak Circumstantial Evidence. (*Qarīnah Dha'īfah)*

The strong circumstantial evidence are the ones which signify strong belief and do not have the possibility of lies in it. Such types of circumstantial evidences are considered a strong source of proof in Islamic law and is advocated by *Qur'an* and *Sunnah*.

Weak circumstantial evidence is not admissible and is not relied upon, unless corroborated by other strong proofs.

As far as the electronic evidence is concerned there are two ways in the Western Law in which circumstantial evidence can be connected to it

1. Electronic crime is proved with the help of physical circumstantial evidence. For instance, in a case *U.S v. Simpsons*, in which the defendant objected that the conversation alleged to be between him and FBI agent, does not belong to him. The court rejected the plea and observed that government authenticated the chat room print outs by a number of circumstantial evidences. For instance, during the discussion in the chat room the defendant gave the name, street number and email address. Later during search of defendant's house, a page was found near his computer containing the email address, street number and telephone number given to the agent.

2. Electronic Evidence is circumstantial evidence itself. Physical crime is proved with the help of circumstantial evidence which is electronic in nature. This can be best illustrated by case, in year 2012, a person named, Christian Aguilar disappeared. He was a friend of Pedro Bravo, both studied at the same University at Florida. Three weeks later, the dead body of Augilar, was found from a grave, 60 miles away from his residence. He was last seen with his friend Bravo. Police suspected Bravo had some relation with the disappearance. After search it was found that he was in possession of Augilar's backpack. There was a reason why Bravo was upset with Aguilar that he had started a relationship with Bravo's ex-girlfriend. Hence, digital evidence made this circumstantial case far more certain. Electronic evidence experts had access to Bravo's cell phone and got many key pieces of proofs. Examiners found out that in the cache for the phone's Facebook app, there was a screen shot of a Siri search made near the time of Aguilar's disappearance that read, "I need to hide my roommate." Determining the tower that received signals from the cell phone, which showed that Bravo had moved far to the west after the disappearance. In the end, examiners were able to investigate that the flashlight app on the cell phone was used for almost one hour after the disappearance. After these evidences and proofs, Bravo was tried in the court, in August 2014. During cross examination he admitted the crime and was convicted of first-degree murder.

The matters in which electronic evidence is the proof itself as a circumstantial evidence to the case, electronic evidence is considered as a very strong proof. These proofs are a centre of attraction for the investigation officers because these proofs cannot be denied. For instance, DNA test, finger prints, Call records, text messages (record of the numbers and timings and on which texts are sent). These are the proofs which cannot be denied by the criminals themselves unless backed by a very strong evidence.

If the nature of the evidence is such that it does not involve human intervention and the system through which it is generated is reliable, such evidence is a strong evidence, even if the evidence is serving as a circumstantial evidence to the crime taken place in the physical world, such as, murder, robbery or terrorism. Such crimes are committed through the help of electronic means. Later on, the calls are traced, the laptops are seized which result in investigation of number of clues. All of these are circumstantial evidence and they play an integral role in investigation.

It is proved that circumstantial evidence has great importance in proving and disproving electronic evidence. Islamic law has relied greatly on circumstantial evidence. *Qur'an*, *Sunnah* and conduct of Companions of Prophet (Peace be upon him) has heavily relied upon strong circumstantial evidence (which are beyond doubt). So, it is automatically proved that electronic evidence for cyber-crimes, which are beyond doubt, would be acceptable in Islamic law and such evidence would be binding in nature. But it must be ensured that nature of the e-evidence must be free of all types of doubts, alterations or errors.

Western law considers circumstantial evidence as strong corroborating evidence for e-evidence. Pakistan law on the other hand, is silent in case of e-evidence dealing in circumstantial evidence.

Islamic law differentiates between *Qarīnah Qātiah* and *Qarīnah Dhaīfa* the first form is an undeniable strongest mean of proof, which is admissible, same is the case with western law also. There is no such distinction present in Pakistani law.

As far as the standards of admissibility in English law are concerned, they are four. The first one them is relevance. The second most important of them is authentication. Authentication is dealt with minute details in Islamic as well as English law. But Pakistani law does not pay much heed towards it.

Like In Islamic law authentication of evidence takes place by a number of ways.

1. Purgation of witness.
2. Testimony by a just witness.
3. Expert witnesses are also not trusted blindly.
4. Documentary evidence is subjected all the procedures of screening for instance, preservation in checked, reliable oral testimony is acquired to accept documentary evidence.
5. Circumstantial evidence is testified by all means and only strong circumstantial evidence is admitted.
6. Knowledge of judge is also utilized where available. It is also for authentication for evidence.

English law has explained through different detailed judgements about the authentication of e-evidence. Like Islamic law, English law also has a number of mean of proof in order to authenticate e-evidence. For instance;

1. Authentication through oral testimony,
2. Authentication through expert testimony,

3. Authentication through circumstantial evidence,
4. Authentication through Hash Tags.
5. Authentication through Meta Data.

As far as authentication of e-evidence in Pakistani law is concerned there are two subsections relating to it;[706]

First of them says that e-evidence is considered admissible if the system be in "working order"

Second one is, authentication of documentary evidence is admissible if the "electronically stored information is unaltered and incomplete, other than the change arise in normal course of communication".

Pakistani law is silent on above mentioned methods of authentication in US and Islamic law with reference to electronic evidence.

Third step of admissibility of electronic evidence in English law is Hearsay. Islamic law has strict standards for following Hearsay. If it is seen closely there is no concept of hearsay in Islamic law. Hearsay is acceptable only in case of death, birth, waqf etc. These are the cases in which news is already spread due to being famous. So, it is not hearsay in its real sense. [707]

Another thing allowed in case of testimony is secondary testimony "*Shahādah* ala *Shahādah*", in which one witness on oath transfer his or her testimony to other. First witness is either out of city, or due to other genuine reason unable to present himself in court that is why he transfers his testimony to another. Witness who then testify in court on oath. This is a safe and sound method of adoption hearsay.

---

[706] See above chap 6, para 6.2.2.
[707] See above chap 2 para 2.3.3.9.1.

English law gives many hearsay exceptions which are free from doubts public documents, business etc. Generally, the standards which are set for admissibility are those in which there are less chances to lie.

Pakistani law states in the last proviso of art 71 that if a witness is unable to come to the court, he can transfer his or her testimony to another witness. This is all it has to say about secondary witnesses. There is no legislation as to what should be the criteria of of witness or what should be the character of witness etc.

The last step of admissibility is original writing rule. This rule is strictly followed in Islamic law in case of physical evidence. In case of electronic evidence, this rule will not apply to the documents which are genuine unaltered, and trust worthy etc.

In US law this rule is abolished in case of electronic evidence. A document which is genuine authentic is an original writing document. Whether it may have many copies. Same is the case with Pakistani law. It also follows original writing rule by only saying that condition of writing and originality does not apply to an electronic document which is genuine and in electronic form.[708]

Electronic evidence is mainly covered by three laws in the Pakistani Law.

a) Qanoon-e-Shahadat Order 1964,
b) Electronic Transaction Ordinance 2002, and
c) Prevention of Electronic Crimes Act 2016.

The cyber laws of Pakistan are not as well versed with the latest trends and technology as the world's laws are. For instance, these laws do not discuss the authentication techniques

[708] See above chap 6, para 6.2.4.

and the rules about Hearsay in electronic evidence. Best Evidence Rule is satisfied in Section 164- of Qanoon-e-Shahadat Order though. [709]

The description given in ETO regarding Electronic Signatures is insignificant and not elaborative. Rather, it is just confined to the permissibility of electronic signatures.[710] Law of other countries, on the other hand, are far more elaborative and well versed with the modern trends and practices.[711]

There are numerous problems in ETO. For instance, it is very brief, general and sometimes ambiguous. It does not cater the needs of e-commerce which is a global phenomenon. Instead it only has a local law.[712] There were a number of amendments done in Qanoon-e-Shahadat Order 1964 through Electronic Transaction Ordinance 2002. However, these amendments too fail to discuss and elaborate numerous matters. For instance;

1. Admissibility of Oral testimony in Electronic Evidence.
2. These laws discuss the computer-generated evidence, but there is no guideline available for computer stored evidence. For instance, there is no guideline regarding the procedure of admissibility and authentication in case of computer stored evidence.
3. Different social media means (such as emails, messages and websites) require different methods of authentication. There is no such discussion on these matters in QSO.

Besides the law, another problem is the judicial system itself. The Judiciary of Pakistan has a very slowly progressing process. The cases registered for cybercrimes are unnecessarily dragged and delayed in courts. The judges and lawyers do not have proper training and they

[709] See above chap. 6, para 6.2.3.1.
[710] See above chap. 6, para 6.2.1.5.
[711] See above chap. 6, para 6.2.1.6.
[712] See above chap. 6, para6.2.1.

cannot work for effective adjudication due to unawareness, making the system even more ineffective.

So far, NR3C in FIA is the only department, working under FIA, that is responsible for dealing with cyber-crimes in Pakistan. But in there, the complaints for cyber-crimes are piled up and unattended, because the number of investigation officers is very low while the volume of complaints is too high. One investigation officer has to deal with more than 700 cyber-crime cases.

7.2 Recommendations

Islamic law strictly stipulates that witness must have just character. The same rule applies to electronic evidence. Testimony for electronic evidence must be taken by a just witness. A witness who has a doubtful character cannot lead to truth.

Purgation of witnesses (secret or public), is another prominent character of Islamic law of evidence. It must take place and should be ensured while admitting testimony for oral evidence in Pakistan. Appropriate legislations for purgation of witness must take place and should be added in Qanun-e-Shahdat Order 1984.

Testimony cannot be given in favour of son, brother, father, or at places where witness has some personal interest, like business partner. Such conditions are totally absent from Pakistani law. It must be added in QSO 1984.

In Islamic law women testimonies are treated differently. Such differences must be ensured in Pakistani law as well. Proper legislation must take place regarding the Islamic standards set for women testimony. These standards are compulsory on Pakistan being a

Muslim country. Whether it be a case of electronic evidence or a physical evidence. Such standards must be legislated.

Islamic law stipulates a number of conditions for the admissibility of oral testimony. These conditions must be legislated in Pakistani law as well. QSO 1984 must be amended accordingly. Number of witnesses for Hudūd and other cases offences as specified by Islamic law, must be legislated in Pakistani law accordingly.

Expert must be two or more in number, just and must be subjected to purgation. One testimony however, is acceptable on the ground of necessity. But this situation is rare in today modern world because more than one expert in the field are easily available.

Standard set for admissibility of circumstantial evidence in classical Islamic law must be incorporated in Pakistani law as well for the admissibility of circumstantial evidence in e-evidence.

Standards set for admissibility of hearsay in Islamic law must be followed in Pakistani law. Secondly, Pakistani law is silent on to deal with electronic evidence which falls under the category of hearsay. Such problems must be addressed by legislations and judiciary.

Proper legislation is required in Pakistan for authentication of electronic evidence. Modern techniques for authentication must be added as well. A separate section should be there to deal with authentication of computer stored and computer-generated evidence. Technological solutions should be given to solve the problem of authentication such as hash tags and Meta data.

Some other measures are required to be taken in Pakistan. The first one of them is to update the existing laws for electronic evidence in Pakistan. The second one of them to make some changes in the infrastructure of judicial and government sector. For instance, there

must be a well-articulated legal system which provides a framework for the intelligence and law enforcement agencies to operate on. The problem is that even though Pakistan has recently legislated PECA and other legislation on this issue, the law still holds no significance because of lack of an infrastructure and system of speedy trials and check and balance.

PECA 2016 is recent legislation. Some offences mentioned in it are non-cognizable which are creating a lot of problems for law enforcement agencies. It should be made cognizable.

Awareness programs must be held for lawyers, judges and the general public so that they cannot be misguided by the lawyers deliberately delaying the suits.

NR3C should be transparent in working. It must have a have strong system of check and balance by the concerned authorities. Ministry of Law and Ministry of IT must collaborate to make the process of registration of complaints, and investigation more transparent instead of lingering on cases for a long time.

It is a need of the hour that Pakistan should sign a treaty of cyber-crime (which is generally known as convention on cyber-crime-CCC). It helps in retrieving data from international jurisdictions. It will also help making Pakistan more reliable in terms of international liaison for dealing with cyber cases and signing MLAT. [713]

The current judicial system of Pakistan must be revised to ensure speedy justice to the aggrieved parties. The judges and lawyers must be trained properly to work speedily in an effective environment. The courts must be fully furnished with all the modern devices which are required for hearing and examination of electronic evidence.

Problem of huge piles of complaints in NR3C should be solved in a way that Computer Emergency Response Teams (CERTS) should be made available all over the country to deal

[713] Mutual legal assistance treaties.

with cyber-crimes instantly. FIA or any other suitable institution should be given complete authority of check and balance over them. The governing body must ensure the safety of citizen's privacy as well. More investigation officers should be hired for NR3C. The process of hearing the complaints should be time lined by different legislations. In case of no-response to complaints, citizens must have some other forums to complaint about NR3C, to which NR3C should be answerable.

Other than that, Pakistan must form a centralised command which can operate as the centralized organization. It will be responsible for the development of defence capabilities in cyber field. The objective of cyber command would be to ensure that Pakistan achieves and keeps a cyber-strategic and cyber deterrent status. China's people's Liberation Army is also working on such a cyber-command, Pakistan can take help from them to develop, keeping in view its deep defensive ties with them. [714]

Additionally, the military, government and private sector must collaborate to develop a framework for securing the country's critical infrastructure. The electronic grid, financial markets, nuclear weapons, private information and other assets of Pakistan must be secure. [715]

The cost of not spending in full spectrum for cyber capabilities will continue to grow as the threat of cyber-attacks will increase potentially in coming future. The upcoming cyber threats cannot be neglected any more. A failure in planning and executing today will cause long term damage to the security of Pakistan.

[714] Uzair. M. Younas. "Threat of cyber terrorism" Dawn. March, 21. 2016. (Accessed: May 9, 2017) https://www.dawn.com/news/1246971
[715] Ibid.

Bibliography

1. Al-Quran.
2. Abū Abdullah, Muhammad al-Fakhr al-Razi. (d. 606) *Mafātiḥ al-Ghayb, al-Tafsīr al-Kbīr* 32 vols. Beirut: Dar Iḥyah al-Turath al-'Arabi, 1420. Also available at : www.altafsir.com
3. Al-Kāsānī, Alā' *al-Dī*n Abū Bakr bin Mas'ud bin 'Aḥmad.(d. 587H), *Badā'i' al-Ṣanā'i fī Tartīb al-Sharā'i.* 2nd ed. 7 vols. Dār al-Kutub al-'Ilmīah, 1998.
4. Al-'Amrī, Ṣāliḥ b. Muḥammad. *Iqāẓ HImām Ūlī-Abṣār li'l-Iqtiḍā' bi-sayyid al-Muhājirīn wa'l-Anṣār.* Beirut: Dār al-Ma'rifa lil-Ṭibā'a wa'l-Nashr, n.d.

5. Al-'Atāsī, Muḥammad Khalid. Sharḥ *Majallah al-Aḥkām al-'Adalīah*. 5 vols. Quetta: Maktabah Islamiah, 1985.

6. Alan, Davidson. *The Law of Electronic Commerce.* New Delhi: Cambridge University Press, 2009.

7. Al-Damishqi, Abdul Mughnī Bin Ṭalib bin Ḥamād bin 'Ibrahīm. *Albāb fī Sharḥ Al-Kitāb*, Beīrūt: Maktabah 'Ilmiah, n.d.

8. Al-Faize, Najah Abdulaziz. "The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia." (2015).

9. Al-Jawziyyah, Ibn Qayyim, and Muhammad bin Abū Bakr. *Al-Turuq al-Hukmiyyah Fi al-Siyasah al-Shar'iyyah.* Cairo: Dār ul-Madni, 1953.

10. Al-Qurtubī, Abū 'Umar Yūsaf bin 'Abdullah. *Al-Kāfī fi Fiqh al-Madīnah*, 2 vols. Riadh: Maktabah al-Riadh al-Ḥaditha: 1980.

11. Al-Nīsābūrī, Muslim Bin al Ḥjāj Abū al-Ḥassan al-Qashīrī, *Saḥīḥ Muslim.* Beīrūt: Dār 'Iḥyīā' Al-'Arabī. n.d.

12. Al-Shaf'ī, Abū Ḥussain Yaḥyah bin 'Abī al-Khaīr al-'Imran. *Al- Bīyān fī-Mazhab Imām Shafaī.* 13 vols. Jaddah: Dār al-Minhāj, 2000.

13. Al-Shīrāzī, Abū Yūsaf. Al-*Muhazab ī al-fiqh al-Imām Shaf'aī*, 3 vols. Dār al-Kitab Al-'Ilmiah, n.d.

14. Al-Sarkhasī, Shamsud-u-Dīn Muḥammad ibn Aḥmad ibn Abī Sahl. *Al-Mabsūt.* 30 vols. Beirut: Al-Ma'rifah Publishers, 1998.

15. Amnon, Cohen. *The Guild of Ottoman Jerushelum.* Boston: Brill, 2001.

16. Mālik, 'Anas bin 'Āmir. *Al-Maūta'*. 6 vols. Abū Ẓahbī: Mūassasah Zahid bin 'Amir al-'Asbīhi, 2004.

17. Al-Zuhaīlī Wahbah, *Al-Fiqh al-Islamī wa 'Adiltuhu.* 10 Vols. Damascus: Dār al-Fikr,1985.

18. Blythe, Stephen E. "Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security." Rich. JL & Tech. 11 (2005): 6-8.

19. Coulson, Noel J. *History of Islamic Law.* Edinburgh: Edinburgh University press, 1964.

20. Dabūr, Anwar Mahmud. *Al-Qara'in wa Dawruhafi al- Fiqh al-Jina'i al-Islami.* Cairo: Dar al-Thaqafah, al-Arabiyyah, 1985.

21. Davidson, Alan. T*he Law of Electronic Commerce.* New Delhi: Cambridge University Press, 2009.

22. Daniel, Larry and Lars Daniel. *Digital Forensics for legal professionals: Understanding digital evidence from warrant to court room.* Waltham: Elsvier, 2012.

23. Delaney, Hayden, and Briar Francis. "Is your use of electronic signatures protecting your interests?." Governance Directions 67, no. 8 (2015).

24. Duranti, Luciana, Rogers, Corinne, And Sheppard, Anthony. "Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later", Arhivaria 70 (Fall 2010); 95-124.

25. _____ "Trust in digital records: An increasingly cloudy legal area", *Computer Law and Security Law Review* 28, (2012): 527

26. Favro, Phillip J. "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata", B.U. J. SCI. & TECH. L 13, no, 1 (2007):1-25. Accessed, May 9, 2017. https://ssrn.com/abstract=2255160

27. Finkelstein, Sheldon M., and Evelyn R. Storch. "Admissibility of Electronically Stored Information: It's Still the Same Old Story." J. Am. Acad. Matrimonial Law. 23 (2010): 45.

28. Fiedler, Betsys. "Are your eyes deceiving you?: the evidentiary crisis regarding the admissibility of computer generated evidence" 48 NYL. Sch. L. Rev. 295, 306 (2003).

29. Fred Galves, "When the not-so-Wild things are Computer in the Courtroom, Federal rule of Evidence and the Need for Institutional Reforms and more Judicial Acceptance", Harvard Journal of Law & Technology 2, Vol 13 (2000); 165-300.

30. Fredesvinda, Insa. (2007), "The Admissibility of Electronic Evidence In Court (A.E.E.C): Fighting Against High-Tech Crime-Result of a European Study", Journal of Digital Forensic Practice, 1:4, 285-289, accessed: May 9, 2017. http://dx.doi.ord/10.1080/1da55 67280701418049

31. Fromhol, Haley J. "Discovery, Evidence, Confidentiality, and Security Problems Associated with the Use of Computer-Based Litigation Support Systems" , 1977 Wash. U. L. Q. 445 (1977). Available at: http://openscholarship.wustl.edu/law_lawreview/vol1977/iss3/10

32. Freider, Jonathan D. and M. Murray. Leigh, "Admissibility of E-Evidence under the Federal Rules of Evidence" Rich.J.L. & Tech 17, no.2 (2011), Accessed: May 9, 2017. http://jolt.richmond.edu/17i2/article5.pdf.

33. Gauthier, Johanne. "The Admissibility Of Computer-Generated Evidence: An Overview" Canadian Maritime Law Associates, November,1997. http://www.cmla.org/papers/Admissibility%20of%20Computer%20Generated%20Evidence.Johanne%20Gauthier.28.Nov.1997.pdf (Last Accessed January 23rd, 2017).

34. Gihanem, Isam. *Islamic medical jurisprudence.* London: Arthar Probsthain, 1982.

35. Goodison, Sean E., Robert C. Davis, and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. RAND Corporation, 2015. http://www.jstor.org/stable/10.7249/j.ctt15sk8v3

36. Haneef, Sayed Sikanadar Shah. "Modern means of proof: Legal basis for its accommodation in Islamic law." Arab Law Quarterly 20, no. 4 (2006): 334-364.

37. Haley J. Fromholz, "Discovery, Evidence, Confidentiality, and Security Problems Associated with the Use of Computer-Based Litigation Support Systems", 1977 Wash. U. L. Q. 445 (1977). Available at: http://openscholarship.wustl.edu/law_lawreview/vol1977/iss3/10

38. Hryko, Oleh. *Electronic discovery in Canada: Best Practices and guidelines*, Edited by Richard Browne B.A. New York: CCH Canadian Limited, 2007.

39. Ibn Nujaīm . Zaīn al-Dīn bin Ibrahīm bin Muḥammd. *Al-Baḥr ar–Rā'iq Sharḥ Kanz al-Daqaiq*, 8 vols. Dār al-Kitāb al-Islāmī, n.d.

40. Ibn Rushd, Abū al-walīd Muḥammad bin Aḥmad. *Bidāyat al- Mujtahid wa nihāyat al-Muqtaṣid*, 4 vols. Cairo: Dār al-Ḥadith, 2004.

41. Ibn 'Ābidīn, Muḥammad Amīn bin 'Umar. *Hāshiyah ibn 'Ābidīn: Rad al-Muḥtār 'Ala al-dār al Mukhtār.* 6 vols. Beīrut: Dār al-fikr, 1992.

42. Ibn Taīmīah, Taqqi-u-din Muḥammad. (d. 728), *Majmū' Fatāwā Shykh al-IRāslām Aḥmad B. Taīmīah, 35* vo ls. Majma' al-Malik Fahad li-Tabā'ah Muṣhaf, 1995.

43. Ingram, Jefferson L. *Criminal evidence.* 12th ed. Waltham: Anderson Publication, 2015.

44. Johanne Gauthier, "*The Admissibility Of Computer-Generated Evidence: An Overview*" Canadian Maritime Law Associates, November,1997.

http://www.cmla.org/papers/Admissibility%20of%20Computer%20Generated%20Evidence.Johanne%20Gauthier.28.Nov.1997.pdf

45. Kerr, Orin S. "Digital evidence and the new criminal procedure." Colum. L. Rev. 105 (2005): 279.

46. Keane, Adrian. and Mckeoron, Paul. *The Modern Law of Evidence.* New York: Oxford University Press, 2014.

47. Krotoski, Mark L. et all "Obtaining and Admitting Electronic Evidence." *United States Attorney's Bulletin* (2011).

48. Leroux, Olivier. "Legal admissibility of electronic evidence 1." International Review of Law, Computers & Technology 18, no. 2 (2004): 193-220.

49. Listrom, Linda L. Harlan, Eric R. Ferguson, Elizabeth H. and Redis, Robert M. "The Next Frontier: Admissibility of Electronic Evidence", Accessed: May 9, 2017. http://www.abanet.org/abanet/ common/login/securedarea.cfm?areaType=premium&role=lt&url=/Litigation/ mo/premium-lt/prog_materials/2007_abaannual/27.pdf (last visited October 20, 2015).

50. Long, Richard M. "The Discovery and Use of Computerized Information: An Examination of Current Approaches." Pepp. L. Rev. 13 (1985): 405.

51. Lydon, Ghislaine. "A Paper Economy of Faith Without Faith in Paper: A Reflection on Islamic Institutional History," Journal of Economic Behaviour & Organization 71, no. 3 (2009): 647-659.

52. Mason, Stephen. et al., *"Electronic Evidence"* 2nd edition. Haryana: LexisNexis, 2012.

53. _____ "Electronic evidence: dealing with encrypted data and understanding software, logic and proof." In ERA Forum, Vol. 15, no. 1, pp. 25-36. Springer Berlin Heidelberg, 2014.

54. *Maūsūa Fiqhiyah al-Qūītīyah*, 45vols. Qūaīt: Dār al-Salāsil, 2006.

55. Mawsilee. Abdullaah al, *Al-Ikhtiyaar Li Ta'leel al-Mukhtaar*, ed. 'Ali Abdul-Khayr and Muhammad Sulaymaan vol. 1. Damascus: Dar al-Khayr Publishers, 1998.

56. Malek, Hodge M. (gen. ed.), *Phipson on Evidence*. 17th ed. Sweet & Maxwell. 2010.

57. Marghīnānī. Burhan al-din Abū Al-Ḥassan 'Ali bin Abi Bakr Farghāni, A*l-Hidāyah* , 4 vols. Beirut: Dar Aḥya Turaṣ al-Arabi, n.d.

58. Meshal, Reem A. *Sharia and the Making of the Modern Egyptian: Islamic Law and Custom in the Courts of Ottoman.* Cairo: Oxford University Press, 2014.

59. Monir, M. *Text book on the Law of Evidence* . New Delhi: Universal Publishing co, 2010.

60. Muḥammad bin Isma'il (d. 256), *Saḥiḥ al-Bukhari*, 9 vols. Al-Najat: Dār al-Tauq, 2001.

61. Najah, Abdulaziz. "The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia," (Ph.D diss., Demonfort University, UK, 2015).

62. Pengilley, Penelope A. "Machine Information: Is It Hearsay." Melb. UL Rev. 13 (1981): 617.

63. Posner, Richard A. "An economic approach to the law of evidence." Stanford Law Review (1999): 1477-1546.

64. Rice, Paul. P. *Electronic Evidence: law and Practice.* New York: ABA Publishing, 2005.

65. Robert, Jerome J. , "A Practitioner's Primer on Computer-Generated Evidence", The University of Chicago Law Review 41(2), 254-280

66. Ross, Margaret L and James P Chalmers. *Walker and Walker: the Law of Evidence in Scotland.* West Sussex: Blooms berry, 2008.

67. Robbins, Ira P. "Writings on the Wall: The Need for an Authorship-Centric Approach to the Authentication of Social-Networking Evidence." Minnesota journal of law, Science and Technology13, no.1 (2013), 193-220.

68. Seng, Daniel KB. "Computer Output as Evidence." Singapore Journal of Legal Studies (1997): 159-166.

69. Shair Mohamed, bin Mohd Akram. "Quantum of proof when case for the prosecution depends substantially or wholly on circumstantial evidence: irresistible conclusion test or reasonable beycnd a doubt test?." Journal of Islamic Law Review 7, no. 1 (2011): 1-35

70. Smith, J. C. "The admissibility of Statements by Computer." Criminal Law Review JUN (1981): 387-391.

71. Stephen Mason, et al. *Electronic Evidence*, 2nd ed. LexisNexis Haryana, 2012.

72. Swift, Eleanor. "Abolishing the Hearsay Rule." Cal. L. Rev. 75 (1987): 495.

73. Teppler, Steven W. "Digital data as hearsay." Digital Evidence & Elec. Signature L. Rev. 6 (2009), 1-13.

74. Turner, Philip. "Digital Provenance – Interpretation, Verification and Corroboration". Digital Investigation 2.1 (2005), 45-49.

75. U.S Government, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal investigations*, (General Books, 2011), Accessed: September 1, 2015. thttp://www.cybercrime.gov/s&smanual2002.htm, October 2004

76. Wakin. Jeanette, *The Function of documents in Islamic Law*. New York: State University of New York press, 1972.

77. Wiley, Jack. et. All. *Techno Security's Guide to E-Discovery and Digital Forensics.* Burlington MA: Elsevier, 2007.

78. Wegman, Jerry. "Computer Forensics: Admissibility of Evidence in Criminal Cases" Journal of Legal, Ethical and Regulatory Issues 8, no. 1/2 (2005): 1-12.