

THE POSITION OF ELECTRONIC EVIDENCE UNDER
ISLAMIC LAW AND MALAYSIAN LAW OF
EVIDENCE

BY

MURSILALAILI BINTI MUSTAPA SA'DI

A thesis submitted in fulfilment of the requirement for the
degree of Doctor of Philosophy

Ahmad Ibrahim Kulliyah of Laws
International Islamic University Malaysia

FEBRUARY 2020

ABSTRACT

In the 21st century, documents are now no longer only on paper and ink but in discs, memory card in computers, smartphones etc. which can be extracted and forwarded to others in tangible and intangible forms, i.e. electronically. The use of electronic document is now so widespread that laws are made to accommodate them. In this era of big data, electronic evidence has been recognised as a form of documentary evidence and laws that govern electronic evidence have been adapted in terms of its authenticity and credibility (weight or its evidential value). As far as Islamic law is concerned, it recognizes documentary evidence as one of the type of evidence. Correspondingly, the earlier Islamic scholars had no opportunities to discuss it in their *fiqh* books. Their definitions of the documentary evidence is about something that can be understood, useful and contain information. From the evaluation, researcher finds that electronic evidence is recognised as documentary evidence from Islamic and Malaysian law perspective. The definition of documentary evidence by earlier Islamic scholars are dynamic and flexible that they can accommodate electronic evidence as a form of documentary evidence. Therefore, electronic evidence subject to the evidentiary rules i.e. best evidence rule, hearsay rule and authentication rule. Discussions from the perspectives of these early Islamic scholars, modern scholars and common law scholars shall be considered/ evaluated/ examined to determine the status of electronic evidence under Islamic law and its reception in today's legal system. The relevance laws pertaining to electronic evidence such as Evidence Act 1950, Computer Crimes Act 1997 and Communications and Multimedia Act 1998 and other jurisdictions applying common laws and Islamic laws are relevant to this research. This research is qualitative research which used data collection and data analysis including library research and semi-structured interview. Findings in this research were used deductively, inductively and comparatively.

خلاصة البحث

في القرن الحادي والعشرين؛ لم تعد المستندات والوثائق ورقية فقط، وإنما رقمية مخزنة في الأقراص وبطاقات الذاكرة في الحواسيب والهواتف الذكية وغيرها، ويمكن استخراجها وإعادة توجيهها إلى الآخرين ورقياً ورقمياً في آن معاً، وشاع استخدام المستند الرقمي حتى سنّت قوانين لضبط هذا الاستخدام، ومن ثم؛ جرى الاعتراف بالأدلة الرقمية شكلاً من أشكال الأدلة الموثوقة يُنظر إليها من حيث صحتها ووثاقتها وأهميتها من منظور قانوني، أما في الشريعة الإسلامية فلم تكن معروفة من قبلُ تقنيةً التواصل الرقمي، ولم تُناقشها المصادر الفقهية؛ لذا يُنظر شرعياً إلى الأدلة الرقمية على أنها نوع من الأدلة الوثائقية، وهذا ما يوافق عليه القانون الماليزي، ويُلاحظ أن التعريف الشرعي للأدلة الوثائقية مرن مفيد لتضمُّنه كثيراً من المعلومات، ويُبيّن أن الدليل الرقمي يخضع لقواعد الإثبات؛ من مثل: قاعدة الأدلة، وقاعدة الإشاعات، وقاعدة التحقق من الأصل، ولكن؛ لا بُدَّ من النظر أكثر في آراء الفقهاء الشرعيين والقانونيين القدامى والمحدثين؛ لتحديد وضع الأدلة الرقمية شرعياً ومدى قبولها في الأنظمة القانونية؛ من مثل: قانون الأدلة 1950، وقانون جرائم الحاسوب 1997، وقانون الاتصالات والوسائط المتعددة 1998، وغيرها من الاختصاصات التي تُطبَّق فيها قوانين عامة وإسلامية في آن معاً، وهذا ما يحاول البحث توكُّيداً من خلال منهج نوعي أداته المقابلات شبه المنظمة لجمع البيانات ذا الصلة، ثم تحليلها ومناقشتها والمقارنة بينها وبين ما ورد في الدراسات السابقة.

APPROVAL PAGE

The thesis of Mursilalaili binti Mustapa Sa'di has been approved by the following:

Abd. Rani Kamarudin
Supervisor

Duryana Mohamad
Co-supervisor

Zulfakar Ramlee
Co-supervisor

Afridah Abas
Internal Examiner

Naim Mokhtar
External Examiner

Ruzman Md. Noor
External Examiner

Erry Yulian Triblas Adesta
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not previously or currently submitted as a whole for any other degrees at IIUM or other institutions.

Mursilalaili binti Mustapa Sa'di

Signature:

Date:

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF
FAIR USE OF UNPUBLISHED RESEARCH**

**THE POSITION OF ELECTRONIC EVIDENCE UNDER
ISLAMIC LAW AND MALAYSIAN LAW OF EVIDENCE**

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

Copyright © 2020 by Mursilalaili binti Mustapa Sa'di. All right reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below.

1. Any material contained in or derived from this unpublished research may only be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposed.
3. The IIUM library will have the right to make, store in a retrieval system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Mursilalaili binti Mustapa Sa'di

.....
Signature

.....
Date

ACKNOWLEDGEMENTS

طه ﴿١﴾ مَا أَنْزَلْنَا عَلَيْكَ الْقُرْآنَ لِتَشْقَى ﴿٢﴾ إِلَّا تَذَكْرَةً لِمَنْ يَخْشَى ﴿٣﴾ تَنْزِيلًا
مِمَّنْ خَلَقَ الْأَرْضَ وَالسَّمَوَاتِ الْعُلَى ﴿٤﴾ الرَّحْمَنُ عَلَى الْعَرْشِ اسْتَوَى ﴿٥﴾

Ta-Ha. We have not sent down the Qur'an to thee to be (an occasion) for thy distress, but only as an admonition to those who fear (Allah), A revelation from Him Who created the earth and the heavens on high. (Allah) Most Gracious is firmly established on the throne (of Authority). (Taha; 1-5)

Alhamdulillah, all praise be to Allah Lord of all World, and Muhammad ﷺ the messenger of Allah in bestowing me this highest academic award that I never dreamt of achieving it. *“Thank you O-Allah for choosing and allowing me to strengthen my Islamic understanding and knowledge with this dissertation as well as making me understands Islam better than before. Please accept this tiny work of mine and be acknowledge as one of my accepted amal o Allah. and further me away from arrogance and ignorance”*.

Special thanks to Public Service Department (PSD), Malaysian Islamic Development Department (JAKIM) & Federal Territory Islamic Department (JAWI), Malaysia for sponsoring my studies and supporting me towards the completion of this doctoral dissertation.

Special thanks also goes to Associate Prof. Dr. Abd. Rani bin Kamarudin the main supervisor of this doctoral dissertation for his supervision, thought, ideas as well as commitment in enabling me to complete my doctoral dissertation, Associate Prof. Dr. Zulfakar bin Ramlee and Assistant Prof. Dr. Duryana binti Mohamad, two co-supervisors of this doctoral dissertation. Assistant Prof. Dr. Afridah binti Abas, the internal examiner of this doctoral dissertation in ensuring this doctoral dissertation is up to the standard as what has been deliberated in the viva voce of this doctoral dissertation where the external examiner are Associate Prof. Dr. Ruzman Md. Noor of Universiti Malaya and YAA Dato' Dr. Haji Naim bin Haji Mokhtar, Chief Syarie Judge of Malaysia as well as the Director General Department of Syariah Judiciary of Malaysia and those whom have been contributing directly and indirectly.

I present and dedicate this work to my parents Haji Mustapa Sa'di bin Haji Ab. Kahar and Hajjah Peredah binti Haji Naim without their unconditional love and support and acceptance, I would never have achieved what I have achieve today. To my parents in-laws Haji Mohamad bin Haji Abdul Kadir and Hajjah Hilaliyah binti Haji Yeop, whom have accepted and treating me and loving me as their own and Hajjah Aminah binti Haji Abdul Kadir my dearest acik, whom I am indebt forever.

My siblings and their respected families, Norfamuzatul Akmar, Mursilylaila, Wardah Abada, Madihah Nur and Muhammad Tazwat as well as my in-laws, Dr. Ahmad Firdaus, Alida Hanum and Ahmad Redzuan.

Last but not least, this work would has not been completed without the understanding, dedications, consideration, sacrifices, and the love of Ahmad Syafiq, Auni Syifaa, Ahmad Raihan, Ahmad Umar, Auni Huda and Ahmad Wildan, *yaa ruuhi wa-hayatii yaa bahjata nafsi wa munaati, unsi fi al-hadhiri wa al-ati, hubbukum yahdini fi al-darbi, wa du'a-i yahfazhukum robbiy.. wa du'a-i yahfazhukum robbiy..*

TABLE OF CONTENTS

Abstract	ii
Arabic Abstract	iii
Approval Page.....	iv
Declaration	v
Copyright Page.....	vi
Acknowledgements.....	vii
Table of Contents	ix
List of Cases.....	xii
List of Statutes	xiv
List of Abbreviations.....	xv
Transliteration Table.....	xvi
CHAPTER ONE: INTRODUCTION	1
1.1 Problem Statement.....	6
1.2 Research Questions.....	8
1.3 Objectives	8
1.4 Hypothesis	9
1.5 Limitation of Research	9
1.6 Research Methodology	9
1.7 Summary of The Chapters	12
1.8 Literature Review	13
CHAPTER TWO: ISLAMIC CONCEPT OF EVIDENCE	26
2.1 Concept of <i>Bayyinah</i> and <i>Shahadah</i>	27
2.2 Type of Evidence in Islamic Perspective.....	30
2.2.1 <i>Iqrar</i> (Admission or Confession).....	30
2.2.2 <i>Shahadah</i> (Testimony).....	32
2.2.3 <i>Al-Yamin</i> (Oath)	35
2.2.4 <i>Al-Qarinah</i> (Circumstantial Evidence)	37
2.2.5 <i>Al-Kitabah</i> (Document).....	40
2.2.6 <i>Al-Ra'yu Al-Khabir</i> (Evidence by an Expert)	44
2.2.7 <i>Al-Qiyafah</i> (Evidence to Establish Paternity)	45
2.2.8 <i>Al-Ilm al-Qadhi</i> (Evidence based on Personal Knowledge of a Judge)	45
2.2.9 <i>Al-Qasamah</i>	45
2.2.10 <i>Al-Li'an</i>	46
2.3 The Requirement of Human Participation/Involvement in Providing Evidence in Legal Matters	47
2.4 Conclusion	50
CHAPTER THREE: NATURE OF ELECTRONIC EVIDENCE	52
3.1 Definition of Electronic Evidence	53
3.1.1 Classification of Electronic evidence.....	56
3.2 Types of Electronic Evidence	58

3.3 Characteristics of Electronic Evidence.....	59
3.3.1 Easily Manipulated or Altered	60
3.3.2 Difficult to Eliminate	61
3.3.3 Metadata.....	62
3.3.4 High Volume.....	64
3.3.5 Recognition of User	65
3.4 Issues Concerning Electronic Evidence.....	67
3.4.1 Authenticity Issue.....	67
3.4.2 Reliability Issue.....	69
3.4.3 Application of Analysing Technique	69
3.5 Conclusion	71

CHAPTER FOUR: PROBATIVE ISSUES CONCERNING ELECTRONIC EVIDENCE AS DOCUMENTARY EVIDENCE.....73

4.1 Concept of Legality	73
4.1.1 Admissibility of Electronic Evidence	75
4.2 Authenticity	92
4.2.1 Form of Authenticating of Electronic Evidence	97
4.2.2 Method in Obtaining Electronic Evidence.....	105
4.3 Reliability	107
4.4 Weightage of Evidence.....	108
4.5 Principle of Relevancy.....	112
4.6 Conclusion	113

CHAPTER FIVE: TREATMENT OF ELECTRONIC EVIDENCE PROBATIVE ISSUE.....115

5.1 Computer Forensic.....	115
5.1.1 Definition of Computer Forensic	116
5.1.2 The Origins of Computer Forensic	120
5.2 The Role of Computer Forensic	123
5.3 Methodology in Computer Forensic.....	124
5.4 Challenges and Legality Aspect of Electronic Evidence in Computer Forensics	127
5.5.1 Expertise.....	127
5.5.2 Costly	130
5.5.3 Internet Architecture	131
5.5 Chain of Evidence: Concept in Ensuring Electronic Evidence Authenticity	131
5.5.1 Concept of Chain of Evidence	132
5.5.2 Definition	134
5.5.3 The Significant of Chain of Evidence.....	135
5.6 Expert Evidence.....	136
5.6.1 Qualification of an Expert.....	136
5.7 Electronic Evidence Integrity	138
5.8 Conclusion	139

CHAPTER SIX: ELECTRONIC EVIDENCE FROM ISLAMIC PERSPECTIVE.....141

6.1 Electronic Evidence from Islamic Perspective.....	142
---	-----

6.2 Islamic Law of Evidence Concept of Legality	144
6.2.1 The Importance of Authenticity	146
6.3 Islamic View on <i>Al-Ra'yu Al-Khabir</i> (Expert Opinion).....	149
6.3.1 Who is an Expert?	149
6.3.2 Islamic Concept of Sanad.....	153
6.3.3 Methodology in Computer Forensic	155
6.4 Conclusion	155
CHAPTER SEVEN: NATURE OF CYBERCRIME	158
7.1 History of Cybercrime	158
7.2 Definition of Cybercrime.....	162
7.3 Cybercrime Characteristic	167
7.4 Cybercrime Issues.....	169
7.4.1 Location of Crime (Crime Scene)	169
7.4.2 Jurisdiction	170
7.4.3 Available Evidence	170
7.4.4 Security	171
7.5 Types of Cybercrime	171
7.5.1 Pornography, Obscene and Offensive Content	172
7.5.2 Identity Theft.....	172
7.5.3 Hacking and Cracking.....	173
7.5.4 Spamming	174
7.5.5 Virus	175
7.5.6 Cyberterrorism	175
7.5.7 Distributed Denial of Service Attack	176
7.6 Conclusion	177
CHAPTER EIGHT: CONCLUSION	179
8.1 Findings	179
REFERENCES.....	184

LIST OF CASES

Alliance and Leicester Building Society v Ghahremani [1992] RVR 198 (Eng Ch Div)
Anvar P.V. v P.K. Basheer and others Civil Appeal No. 4226 of 2012
Antoine Levar Griffin v State of Maryland No. 74, September Term, 2010; 419 Md. 343; 19 A.3d 415; 2011 Md. LEXIS 226
Armstrong v. Bush, 721 F. Supp. 343, 345 n.1 (D.D.C. 1989)
Armstrong v. Executive Office of the President, 1 F.3d 1274, 1280, 1283 (D.C. Cir. 1993)
Asian Corporate Services (SEA Pte Ltd v Eastwest Management Ltd (Singapore Branch) [2006] 1 SLR 901
Avnet Azure Sdn. Bhd. v Eact Technologies Sdn. Bhd. and Sapura Research Sdn. Bhd. [2011] MLJU 937
Bank Pembangunan Malaysia Berhad [Company No.16562-K] v Sasacom Sdn Bhd [Company No,146522-U] [2010] MLJU 1402
Borneo Co (M) Sdn. Bhd, v Penang Port Commision [1975] 2MLJ 204
Datuk Seri Anwar bin Ibrahim v Wan Muhammad Azri bin Wan Deris [2014] MLJU 177, 9 MLJ 605
Daubert v. Merrell Dow Pharmaceuticals 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)
DPP v McKeown; DPP v Jones [1997] 1 All ER 737
Eddyham bin Zainuddin v Rahimah bt. Muhamad (2015), 40(2) JH 238 (Syariah Appeal Court Negeri Sembilan)
Fredrick Thomas Saturley v. CIBC World Markets Inc. [2012] N.S.J. No. 313
Gavin Goodale & Ors v. Ministry of Justice & Ors [2010] EWHC B41 (QB).
Ghazali bin Salleh & Anor v PP [1993] 3 CLJ 638
Gnanasegaran a/l Pararajasingam v Public Prosecutor [1997] 3 MLJ 1 (CA)
Grant v Southwestern and County Properties [1974] 2 All ER 465.
Hanafi Mat Hassan v PP [2006] 4 MLJ 134
Hill v. R [1945] 1 KB 329
Jet Holding Ltd and Others v Cooper Cameron (Singapore) Pte Ltd and Another [2005] SGHC 1494, SLR 417
Kennedy v Baker [2004] FCA 562
Lim Mong Hong v Public Prosecutor [2003] SGHC 161
Patrick Collins, Inc. v John Doe 945 F. Supp. 2d 367; 2013 U.S. Dist. LEXIS 71122
Petroliam Nasional Bhd & Ors v Khoo Nee Kiong [2004] 2 LRC 202
PHE, Incorporated dba Adam & Eve v Department of Justice 139 F.R.D. 249 (D.D.C. 1991)
PP v. Muhammad Nuzaihan bin Kamal Luddin [2000] 1 S.L.R. 34; [1999] SGHC 275
PP v Azilah Bin Hadri and Another Criminal Appeal No. 05-185-09/2013(B), Federal Court
Public Prosecutor v Dato' Seri Anwar Ibrahim (No 3) [1999] 2 MLJ 1
PP v Law Aik Meng [2007] 2 814, [2007] SGHC 33
PP v Mohd Abdul Azizi bin Ibrahim [2013] MLJU 530
PP v Sow Kuen Chun Criminal Case No: 63-01-2008
PP v Muslim [2013] 1 AMR 436.
PP v Goh Hoe Cheong & Anor [2006] MLJU 468

Patrict Breyer v Bundesrepublik Deutschland C-582/14, EU Cases/Court of Justice of the European Union/2016/CJEU 19.10.2016
Mohammad Sulasi bin Mohamad and Johari bin Talib, Reference fail: UPK:290-1/2002, dated 112/2002
Mohd Ali Jaafar v Public Prosecutor [1998] 4 MLJ 210
Moriazi bin Mohamad v Ajmawati bte Attan [2005] 4 SHLR 108
Nadhimuthu v. PP [1974] 1 MLJ 20
National Justice Compania Naviera SA v Prudential Assurance Company Limited, 6 [1993] 2
N.C.T. of Delhi v Najvot Sandhu [2005], 11 SCC 600
R v Daye [1908] 2 KB 333
R v Maqsd Ali, R v Ashiq Hussain [1965] 2 All ER 464
R v Petersen (1983), 45 N.B.R. (2d) 271
R v Rahkola, [1979] 5 W.W.R. 464
R v Vallor 2003] EWCA Crim 2288
R v Wood, (1982) 76 Cr App Rep 23
Senior v Holdsworth [1976] Q B 23; [1975] 2 All ER 1009; [1975] 2 WLR 987
The People of the State of New York v Karon Lenihan, [2008] 30 Misc. 3d 289
State of North Carolina v Michelle Catherine Theer, No COA05-1640. Court of Appeals of North Carolina
State v. Taylor and The North Carolina State Bureau of Investigation Lab Scandal 1991
Subramaniam v PP [1956] 22 MLJ 220.
The People of the State of New York, v. Victor Garcia, Rafael Morel and Kennedy Tabares 170 Misc. 2d 543; 647 N.Y.S.2d 355; 1996 N.Y. Misc. LEXIS 333
Teoh Hoe Chye v Public Prosecutor and Yeap Teong Tean v Public Prosecutor, [1987] MLJ 220
West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999).
Wong Chop Saow v PP, [1965] 1 MLJ 247
YB Dato' Haji Husam bin Hj. Musa v Mohd Faisal bin Rohban Ahmad, Civil Appeal No: D-02-1859-08/2012
Zainab binti Mahmood v Abd. Latif bin Jusoh, (1993) Jurnal Hukum (JH), 297
Zainul Abidin bin Mat Akhir v Ahmad Nazreen bin Zainul Abidin & Others (2016), 43(1) JH 17 (Syariah Appeal Court Kuala Lumpur)

LIST OF STATUTES

Computer Crimes Act 1997 (Act 563) (Malaysia)
Communications and Multimedia Act 1998 (Act 588) (Malaysia)
Civil Evidence Act 1968 (United Kingdom)
Criminal Justice Act 2003 (United Kingdom)
Computer Misuse Act 1993 (Singapore)
Criminal Procedure Code (Act 593) (Malaysia)
Criminal Procedure Code 1873 (India)
Defamation Act 1957 (Act 286) (Malaysia)
Digital Signature Act 1997 (Act 562) (Malaysia)
Electronic Commerce Act 2006 (Act 658) (Malaysia)
Evidence Act 1995 (Australia)
Evidence Act 1950 (Act 56) (Malaysia)
Evidence Act 1872 (India)
Evidence Act 1872 (Singapore)
Evidence Act (Nigeria)
Evidence Act (Canada)
Evidence (Amendment) Act 1993 (Malaysia)
Federal Rules of Evidence (US)
Information Technology Act 2000 (India)
Penal Code (Act 574) (Malaysia)
Police and Criminal Evidence Act 1984 (United Kingdom)
Prevention of Corruption Act 1961 (Malaysia)
Specific Relief Act 1950 (Act 137) (Malaysia)
Syariah Court Evidence (Federal Territories) Act 1997 (Malaysia)
Syariah Court Evidence (Perak) Enactment 2004, Enactment No.8 of 2008 (Malaysia)
Youth Justice and Criminal Evidence Act 1999 (United Kingdom)

LIST OF ABBREVIATIONS

CCA	Computer Crime Act
CMA	Communications and Multimedia Act
CLJ	Current Law Journal
DDoS	Distributed denial of service
EA	Evidence Act
ESI	Electronic Store Information
EWCA Crim.	England and Wales Court of Appeal (Criminal Division)
FRE	Federal Rule of Evidence
Ibid.	Ibidem
IIUM	International Islamic University Malaysia
JH	Jurnal Hukum
MLJ	Malayan Law Journal
MLJU	Malayan Law Journal (Unreported)
Ors.	Others
Ph.D	Doctor of Philosophy
PP	Public Prosecutor
R.	Rex
SLR	Singapore Law Report
SHLR	Shariah Law Reports
v	Versus
Vol.	Volume

TRANSLITERATION TABLE

ء	ا	خ	kh	ش	sh	غ	gh	ن	n
ب	b	د	d	ص	ṣ	ف	f	هـ	h
ت	t	ذ	dh	ض	ḍ	ق	q	و	w
ث	th	ر	r	ط	ṭ	ك	k	ي	y
ج	j	ز	z	ظ	ẓ	ل	l		
ح	ḥ	س	s	ع	ʿ	م	m		

Short Vowels		Long Vowels	
ا	a	ا+	ā
ي	i	ي+	ī
و	u	و+	ū

CHAPTER ONE

INTRODUCTION

BACKGROUND OF THE RESEARCH

In both civil and criminal cases, for the court to make decisions, the evidence must not only be legally relevant to be admissible, it must also be weighty (credible) or otherwise it will need corroboration. The evidence admitted may be in oral or documentary. Nowadays, often then not; documentary evidence is electronically generated or transmitted. This is because, human ways of life are followed closely by technological advancements. Previously, humans can only dream of looking at their loved ones when talking in an enclosed area within a building, not to mention across town or even continents. Before the introduction of internet, computers, smartphones, memory card, and thumb drives etc., documents could only be received not instantaneously. However, nowadays documents could be viewed and received in a matter of seconds through Instagram, Multimedia messaging service (MMS), Short Message service (SMS) or WhatsApp Messenger (WhatsApp) to name a few of them. Humans could even do purchases and banking transactions while located far away from the nearest shop or financial institutions. Before this, all of the above activities could only be possible through human physical interactions.

With the emergence of the Internet, activities could also be successfully conducted online or electronically. These elimination of the physical barriers have been made possible as early as in middle 1990, where the Internet has had a drastic impact on human culture and commerce, through the introduction of almost real-time (near-instant) communication that are, electronic mail, instant messaging, Voice over Internet

Protocol (VoIP) "phone calls", two-way interactive video calls, and of course the World Wide Web or www for short, with its discussion forums, blogs, social networking, and online shopping sites. The Internet continues to grow, and drive the world economy to a level where communications etc. are no longer a big deal.

The Internet seems to create a world within a world, that eliminates all geographical and political boundaries but virtual in nature. Nowadays, countries are depending more on innovative information technology in administering almost every aspect of daily life, ranging from ID cards, credit cards, cash card, toll card to health records or the security and defence of its borders¹.

As human life's advances, more and more electronic gadgets or devices are being used and developed not only to lessen the burdens of every day human chores, but also to safeguard human's life, making human becoming more and more dependent on electronic gadgets especially smart phones. With the use of e-mails, for example, documents and correspondence is much faster and more efficient than before. Closed Circuit Television or CCTVs are becoming the eyes of law enforcement in ensuring safety and in safeguarding the nation. There are many CCTVs along highways and traffic lights. These devices or instruments generate and store electronic evidence and these electronic evidence are adduced at the trial of an accused. Cellular phones nowadays not only are being used as conversation tools, but also as data and text relaying devices. Those are amongst the few electronic devices and applications (software) which are being widely used to keep data as evidence.

Unfortunately, with all the advantages that the internet brought, it has also been utilized in strengthening traditional criminal activities, as well as fostering new one.

¹ Misbah Saboohi, "Collecting Digital Evidence of Cyber Crime" (paper presented at the International Judicial Conferences, organized by Supreme Court of Pakistan, 11-14 August 2006).

Through the Internet, criminals are now expanding their activities across geographical and political boundaries. These novel criminal activities are famously known as cybercrime. Cybercrime refers to any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment². Cybercrime would be “unlawful acts wherein the computer is either a tool or a target or both”³. Cybercrime also can be known as internet crime or electronic crime or computer crime. When cybercrime is involved, the evidence normally is in the form of electronic evidence related and associated with the internet, computers and other electronic devices. This form of documentary evidence is also known as electronic evidence or digital evidence or computer evidence⁴.

Due to the nature of cybercrime itself, which is internet based, borderless, international character, easy access, chaotic structure and anonymity⁵ characteristics of the criminal activities, as well as the virtual in nature, it is difficult for cybercriminal to be prosecuted either because they are not in the jurisdictions but also linking the evidence to them may be filmsy. Proving cybercrime is no different as proving the commission of sorcery in the sense the evidence tends to be elusive and intangible. However, this thesis is not on cybercrime but on reception of electronic evidence under Islamic law as far as documentary evidence is concerned. Nevertheless, to elucidate what is electronic evidence, a chapter on cybercrime is allocated.

² United Nation, “Crimes Related to Computer Networks”, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000.

³ Nagpal. Rohas, *Evolution of Cyber Crimes*, (Asian School of Cyber Laws, 2008), 2.

⁴ Brenner, Susan W, “Cybercrime Metrics: Old Wine, New Bottles?”, *Virginia Journal of Law & Technology*, vol. 9, no 13, (2004): 11.

⁵ Yariv Tsfati & Gabriel Weimann, “Terror on the Internet”, *Studies in Conflict & Terrorism*, vol. 25, no. 5, (2002): 317.

Currently, the volume of electronic evidence continues to mushroom unabated as individuals increase their e-mail usages as their means of communication in lieu of the telephone⁶. Electronic evidence also comprises between thirty and seventy percent of all evidence in litigation matters, while other findings⁷ as much as thirty percent of all evidence is maintained in electronic form. As the Internet and e-mail grow in importance in the daily lives of potential clients and their counsel, statutory and case law in this area will expand⁸.

Before any evidence could be accepted in any courtroom, the evidence first, needs to be adduced in court. Before any evidence could be adduced in court beside relevancy, it needs to have certain criteria of authentication or verification. Vacca⁹ states that there are five rules of collecting electronic evidence. These five rules relate to five properties that evidence must have to be useful, which are admissible, authentic, complete, reliable and believable. Therefore, in ensuring the principle of justices are being served, by means of protecting the innocent and penalizing the guilty, electronic evidence presented and admitted and used in court to determine the innocent and guilty of a party must be authenticated.

⁶ Jokela, Lynn, "Electronic Discovery Disputes: Will the Eighth Circuit Courts Move beyond Ad-hoc Decision Making?", *William Mitchell Law Review*, vol. 30, no. 3, Article 7, (2004): 1031. Academic Search Premier, via William Mitchell Law Review, <<http://open.mitchellhamline.edu/wmlr/vol30/iss3/7>>.

⁷ Keena, JR, quote Monte E. Sokol & Phillip P. Andriola, "Cyberspace Becomes Ground Zero in Discovery Process and at Trial," *N.Y.L.J.*, in *E-Discovery: Unearthing Documents Byte by Byte*, Minnesota State Bar Association, <http://www.mnbar.org/benchandbar/2002/mar02/ediscovery.htm> (accessed 14 September, 2012).

⁸ Ungar, Steven and Foldes, Katherine, "Electronic Evidence: Issues Arising in Domestic Relations Cases", (paper presented at Family Law Odyssey, Oregon State Bar Family Law Section's Annual Conferences organized by Oregon State Bar Family Law Section, Oregon, United States, November, 2001).

⁹ Vacca, John R, *Computer Forensics Computer Crime Scene Investigation*, (Boston, Massachusetts: Charles River Media Inc., 2nd Edition, 2005), 220.

In order to prove in civil or criminal cases, it requires evidence that is relevant¹⁰, and authentic¹¹. In oral evidence, authentic in the sense the evidence given is direct evidence not a hearsay evidence. Likewise, in documentary evidence, authenticity is in the sense that it is primary evidence and has been authenticated. Electronic evidence is not free from criticisms particularly concerning its accuracy and authenticity of its contents. Electronic evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination¹². The main issues for establishing the admissibility of electronic evidence is a deep distrust of its reliability and authenticity, due to surveillance techniques are untrustworthy as there remain chances of manipulation¹³. Moreover, a manipulated datum or photograph or information is not admissible as evidences. Thus, to overcome this legal epidemic, certain provisions were inserted to ensure the genuineness of electronic evidence by necessitating that it be first authenticated before determining the truthfulness of its contents. For example sections 90A, 90B, and 90C of the Malaysian Evidence 1950 (Act 56) were inserted to govern the admissibility of electronic evidence.

Islamic law is not an exception and one who is familiar on the book of *hadith* will come across a collection by *hadiths* collectors such as Sahih Muslim and Sahih Bukhari. *Sahih* means authentic. Giving all the issue with regard to electronic evidence, Islamic law of evidence stresses that in admitting evidences, first and foremost, evidences must be authentic, valid and legal, as mention by Allah SWT¹⁴ to judge

¹⁰ Evidence Act 1950 (Act 56), section 5.

¹¹ Evidence Act 1950 (Act 56), section 67 to 90.

¹² Ashcroft, John, Daniels, Deborah J. and Hart, Sarah V., "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", National Institute of Justice Report, (April, 2004) <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf> (accessed 22 January, 2013).

¹³ Radhakrishna, Gita, "E-Mail Evidence and the Hearsay Rule -Commentary on a Recent Malaysian Case," *Digital Evidence & Electronic Signature Law Review*, vol. 10, (2013): 114; Abu Hena Mostafa Kamal, "Admissibility of Surveillance. A Legal Perspective", *ASA University Review*, vol. 2, no. 2, (2008): 30.

¹⁴ An-Nisā: 105.

people justly. Therefore, without authentic, valid and legal evidence will lead to unfairness in verdict indeed *maqasid al-syariah* is unachieved in society.

The concept of authenticity and validity are also explained by Allah's messenger Prophet Muhammad SAW¹⁵. Therefore, in admitting evidence at a trial, it needs to be authentic to be credible i.e. reliable in terms of its evidential value. Any evidence that is false and doubtful must be ignored because there are not authentic hence not credible. The authenticity of the traditions of the prophet will be discussed in chapter six.

The importance of authenticity under Islamic law for a document is similar with the concept of the best evidence rule in Malaysian's Evidence Act (Act 56) which requires primary evidence¹⁶ and to be authenticated¹⁷. In other words, among others, the maker must be called or otherwise to call the witness or it will be hearsay evidence. The issues, therefore, where the document is electronically generated, how it is to determine that it is authenticate and credible? Therefore, this study also needs to determine the Islamic view on the reception of electronic evidence and whether Islamic law considers electronic evidence as documentary evidence. The definition of documentary evidence under Islamic law that is *kitabah* needs to be examined.

1.1 PROBLEM STATEMENT

Question on the position of electronic evidence under Islamic Law of Evidence create a large lacuna where these issues need to be addressed. The nature of electronic

¹⁵ Related by al-Bukhāri and Muslim in hadith: "The *halal* is clear and the *haram* is clear, and between them are matters unclear that are unknown to most people. Whoever is wary of these unclear matters has absolved his religion and honour. And whoever indulges in them has indulged in the *haram*. It is like a shepherd who herds his sheep too close to preserved sanctuary, and they will eventually graze in it. Every king has a sanctuary, and the sanctuary of Allah is what He has made *haram*. There lies within the body a piece of flesh. If it is sound, the whole body is sound; and if it is corrupted, the whole body is corrupted. Verily this piece is the heart." Ṣaḥīḥ al-Bukhāri 52, Ṣaḥīḥ Muslim 1599.

¹⁶ Evidence Act 1950 (Act 56), section 64.

¹⁷ Evidence Act 1950 (Act 56), section 67-73.

evidence itself somehow restrict its acceptance and admission under the Islamic Law of Evidence, where it has the characteristics of being fragile, brittle, easily manipulated and forged, the chain of custody are quite difficult to established.

Electronic evidence can be considered as a new type of evidences due to ongoing revision and amendment of evidence and evidence related Acts across the world, whereby the amendments and revisions are trying hard to accommodate this novel evidence without question and doubt to be utilised in court proceedings. The emergence of the electronic evidence has somehow created a big hole in Islamic Law legal literature whether it is accepted as evidence or only as an aid to investigation. The position of electronic evidence requires a further and detail research on its position, acceptance and the admissibility under Islamic Evidentiary Principles.

Difficulties arises in prosecuting criminals and cyber criminals when utilizing electronic evidence are due to the nature of electronic evidence which are intangible, unseen, fragile, existed mostly in digital format which requires further treatment through forensic computing and sometimes are doubtful, unreliable and unauthentic

This is due to electronic evidences itself differs from that of traditional evidences because it is easily manipulated, easily erased or deleted and quite untraceable or not easily traced by nature and characteristics. Electronic evidence itself is easily manipulated and therefore its authenticity is questionable because access to the computer and internet such as Wi-Fi, broadband registered users easily give away their password. Apart from issues relating to authenticity due the fragile¹⁸ nature of electronic evidence, the internet itself acknowledges a person as Internet Protocols (IP) address

¹⁸ Radhakrishna, Gita, "Legal Issues in Electronic Evidence", *Malayan Law Journal Articles*, volume 4, (2009): lxxii.

and not the person himself ¹⁹ i.e. by names and physical physique. With the ability of humans creativities, stealing IP address is like “taking a cake from a baby” by even amateur hackers, not to mention the electronic data that could be modified accordingly by the hackers to fulfil certain purposes. Apart from availability of evidence, the issues concerning the evidences itself plays a significant role in successfully prosecuting the cyber criminals/offenders. Therefore, the utilization of electronic evidences in establishing and prosecuting cybercrimes requires further scrutiny and verification of its authenticity and validity.

1.2 RESEARCH QUESTIONS

1. What are the positions of electronic evidence under Islamic Law of Evidence?
2. What are the issues to ensure acceptance and admissibility of electronic evidence in court?
3. What is the role of expert opinion testimony in proving electronic evidence?

1.3 OBJECTIVES

The objectives of this research are: -

1. to examine the admissibility and acceptability of electronic evidence under both Islamic and Malaysian Law.
2. to provide guidelines in determining electronic evidence that could be classified as evidences according to Islamic law of evidence.

¹⁹ Chen, Yinjie and ors., “Identifying Cyber Criminals Hiding Behind Wireless Routers”, (paper presented at Conference IEEE International Conference on Computer Communications Workshop (Infocom) organized by IEEE Infocom, Shanghai, China October 2011).