SECURING ONLINE EVIDENCE IN CIVIL CASES: THE LEGAL PERSPECTIVES

DURYANA BT MOHAMED
LLB(HONS), LLB(HONS) (SHARIAH), LLM, ADVOCATE & SOLICITOR, HIGH COURT OF MALAYA (NON-PRACTISING)
AHMAD IBRAHIM KULIYYAH OF LAWS, INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

ABSTRACT: Evidence is very important in establishing and proving any cases. Generally, only reliable and authentic evidence is admissible in the court of law. In civil cases such as online defamation and online breach of data or confidential information parties are required to establish their case on the balance of probabilities. This means, in order to succed in civil action against the defendant the plaintiff shall establish that there is a cause of action against the defendant. For instance, there is evidence that the defendant has uttered defamatory statement and the statement is published widely. In this situation, the plaintiff needs to produce good and reliable evidence either by oral submission or by written statement. However, before producing such evidence both parties need to know the appropriate methods of securing online evidence. If there is lack of care, the evidence may be lost, tampered or deleted during the process of securing such evidence. This paper will discuss on the methods of securing online evidence and their position under the Malaysian laws and procedures. (172 words)

KEYWORDS: *evidence, online, information, methods, civil action*

INTRODUCTION

Online evidence is admissible in the court of law provided it fulfills the requirements of the law of evidence. This evidence can be obtained from cases that involve internet such as online defamation and online breach of data or confidential information. In order to succeed in these cases, the plaintiff must provide relevant and reliable evidence to establish his cause of action against the defendant and he must proof the case on the balance of probabilities. In online defamation, for instance evidence must be shown that the defendant has uttered defamatory statement and the statement was published online. The parties must also know the relevant laws and procedures in securing online evidence. If there is lack of care, the evidence may be lost, tampered or deleted during this process. Securing online evidence can be discussed from different perspectives. From technical perspective, securing online evidence is done by using appropriate softwares and procedures employed by forensic expert. While from legal perspective, online evidence can be secured or acquired by applying several methods available under civil procedural law and criminal procedural law. This paper will focus on securing online evidence in civil cases based on civil procedural law. Relevant laws on securing or protecting online evidence will also be referred to.

MEANING OF SECURING ONLINE EVIDENCE

The word 'secure' has different meanings depending on type of cases or situations. In the context of this paper 'securing' means 'getting or obtaining or acquiring'. Securing evidence is used in *Mohd Za' ba bin Abdul Talib & Anor* v *Public Prosecutor*[1] where evidence of an agent provocateur is admissible eventhough he abets the comission of crime. It is because according

[1] [2013] MLJU 252

to section 40A of Dangerous Drugs Act 1952. '……..no agent provocateur shall be presumed to be unworthy of credit by reason only of his having attempted to abet or abetted the commission of an offence by any person under this Act if the attempt to abet or abetment was for the sole purpose of securing evidence against such person.'

The word 'online' refers to 'Computer or device connected to a network (such as Internet) and ready to use (or be used by) other computers or devices; Database, file, or webpage available for downloading or reading or services such as ticket resevation system, or capability such as online help, available directly through a computer sytstem or under its direct control.'(Business Dictionary.com) Database is described as "quantity of data available for use, which is stored in a computer in a way that enables people to get information out of it very quickly".[2] Examples of databases on the internet include alphabetical lists of names and addresses and lists of hypertext links and website addresses. [3] The database or file may contain relevant information which can be used as evidence. In UK, the civil courts decided that a computer database containing relevant information is considered to be a 'document'(see *Derby v Weldon (no.9)* [1991]1 WLR 652 and *Alliance & Leicester Building Society* v *Ghahremani* (1992) 32 R VR.138). File is a collection of related data or program records stored on some input/output or auxiliary storage medium.[4] While webpage is a single, usually hypertext document on the World Wide Web that can incoporate text, graphics, sounds etc.[5] Metadata is another type of online evidence. It resides and hidden in the computer.

Based on the above definitions, 'securing online evidence' in this paper can be defined as 'getting or collecting database, file or webpage which is available for downloading or reading in computers or other electronic devices'.

ADMISSIBILITY OF ONLINE EVIDENCES

According to section 3 of the Evidence Act 1950, evidence includes-

(a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence;

(b) all documents produced for the inspection of the court: such documents are called documentary evidence;

The above definition divides the type of evidence into oral and documentary evidence. The statement is not only refers to statement under oath but also include statement by an accused from the dock.[6] Generally, evidence must be relevant to the fact at issue and reliable. Section 5 of the EA 1950 provides that, 'Evidence may be given in any suit or proceeding of the existence or non existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others'. But the admissibility of evidence could be challenged by attacking the weight or reliability of the evidence.[7] In this circumstance, the court is under a duty to disallow all inadmissible evidence or to readmit evidence after having rejected it or may reverse

---

2 Collins Cobuild English Dictionary, Scotland: Collins Publisher. 1996

3 Susan Singleton, Business, the Internet and the law, Tolley's: United Kingdom,1999, Chapter 3 at 65.

4 http://www.dictionary.reference.com

5 http://www.dictionary.reference.com

6 Augustine Paul, *Evidence: Practice and procedure*, second edition, Malayan Law Journal, 2004 at 17.

7 Michael Chissick (ed) and Alistair Kelman, '*E-commerce: Law and Practice'*, 3rd edit, A Thompson Company, Sweet & Maxwell Ltd., 2002 at 192.

its ruling on admissibility.[8] Database, file and webpages will become evidence if they fulfill the above criterias namely, relevant, reliable and authentic. But the above section must be read with section 136(1) of the EA 1950. Section 136 provides that the court has power to decide on the admissibility of the evidence and its relevancy to the case in issue.[9] Further, sections 6 to 55 of the EA 1950 mention about the facts declared to be relevant.[10] However, there are exceptions to this rule. In *R* v *Turner* [1975] 1 All ER 60, at 74 (CA), Lawton LJ stated as follows, 'Relevance, however does not result in evidence being admissible: it is a condition precedent to admissibility'. If data is tainted or tampered by someone irresponsible the data shall not be admissible as evidence. For companies, data is regarded as a source of information and priceless in nature. If any of the employees fails to ensure safety and security of company data he will be liable for breach of confidential information.

In addition, the law of evidence also provides certain conditions for data or evidence to be admissible. For example, the tape recording must be played over in court before it can be admitted in evidence. It is admissible upon being tendered through its maker after proof of the required matters.[11] Since online evidence is very fragiled and easily being tampered one must be careful in handling and securing this evidence. Any act of negligence may also break the chain of evidence.

PROTECTING ONLINE EVIDENCE

Online evidence or data needs security protection in order to maintain its authenticity. For companies, it is very important to protect security of their online data. This can be done in many ways such as keeping computers and associated components out of public view, enforcing restrictions on internet access, ensuring that the company's anti-malware solution is up to date and fighting off hacking attacks with intrusion detection technology. These are among the methods suggested to secure data online.[12]In e-commerce transactions, a secure electronic transaction (SET) is used to provide secure payment using credit cards. SET protects payment information based on authentication (merchants & cardholders authentication) and encryption of payment information, which is basically similar to Secure Socket Layer (SSL). SSL is a security protocol developed by Netscape Communications to protect communication over the Internet.[13]

A company that sells products via websites and accept payment by credit cards should be more cautious. They are supposed to maintain data integrity and security as to protect the information from being stolen. If for instance, the company's server was hacked and the consumer's credit card data was stolen the company or the seller would be responsible for such negligence act. This incident may result with legal action by the consumer who has suffered lost.[14]

---

8 Augustine Paul, n.6 at 35-38.

9 *Public Prosecutor* v *Dato' Seri Anwar bin Ibrahim (no 3)* [1999] 2 MLJ 1, 170 (HC) and Augustine Paul, n.6 at 27-28.

10 Augustine Paul, *n.6*, at 29.

11 *Mohd Ali Jaafar v Public Prosecutor* [1998] 4 MLJ 210.

12 Oracle Database + 2 days: security Guide, 2011 at …. See also Top 10 ways to secure your stored data http://www.computerworld.com/s/article/9002188/Top_10_ways_to_secure_your_stored_data retrieved 2 July 2014

13 Mohammad Nabil Almunawar, Securing electronic transactions to support e-commerce,(July 2012) retrieved July 2 2014. http://arxiv.org/abs/1207.4292

14 Roger LeRoy Miller & Gaylord A. Jentz, Management and e-commerce: The online legal environment, US: West Thomson Learning, 2002 Chap8 175-200 at 176

SECURING ONLINE EVIDENCE: THE LAWS AND PROCEDURES

Securing online evidence also involves understanding on the relevant laws that regulate online data security. In Malaysia, there are two relevant laws that deal with data security namely, Digital Signature Act 1997 (DSA) and Personal Data Protection Act 2010 (PDPA). DSA came into force in October 1998.[15] According to this Act, 'Digital signature " means a transformation of a message using an asymmetric crytosystem such that a person having the initial message and the signer's public key can accurately determine —

(a) whether the transformation was created using the private key that corresponds to the signer 's public key; and
(b) whether the message has been altered since the transformation was made;

"Aysmmetric cryptosystem " means an algorithm or series of algorithms which provide a secure key pair. Digital signature is used for cryptographic signature methods and "electronic signature" is used for other paperless signature methods. Cryptography is the science of securing information. It is most commonly associated with systems that scramble information and then unscramble it. Security experts currently favor the cryptographic signature method known as Public Key Infrastructure (PKI) as the most secure and reliable method of signing contracts online. PKI uses an algorithm to encrypt online documents so that they will be accessible only to authorized parties. The parties have "keys" to read and sign the document, thus ensuring that no one else will be able to sign fraudulently. [16] By using digital signature or crytographic signature it provides a secured online payment in e-commerce transactions. But the major challenge to encryption-based security is cryptoanalysis, an activity to break the encryption by guessing keys.[17]

In US, Electronic Signatures in Global and National Commerce Act (ESIGN Act) allows parties to enter into e-contracts.[18] It confirms the legal effect of online transactions and allows consumers to choose either to do online transactions or in paper form. [19] DSA and ESIGN also allow online evidence to be produced in court as long as the evidence is relevant and authentic.

PDPA 2010 is an Act that provides security and protection to personal details of data subject. The Act which is applicable to all personal data in respect of commercial transactions would cover online sales involving blogs. Most sales would involve the collection of personal names, addresses, phone numbers, Identification Card numbers and the like, all of which would be classified as personal data as they relate directly to the data subject and identifiable to the person concerned.[20] Under this Act, any personal data would be subjected to seven privacy principles, i.e.:

---

15 Utah in the US was the first state to enact a digital signature law in 1995. ESIGN Act was signed by President Bill Clinton in 2000.

16 http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html

17 Mohammad Nabil Almunawar,n.13

18 Sylvia Mercado Kierkegaard, *E-Contract Formation: U.S. and EUPerspectives*, 3 Shidler J. L. Com. & Tech. 12 (Feb. 14, 2007), *at* http://www.lctjournal.washington.edu/Vol3/a012Kierkegaard.html

19 Robert A.Wittie & Jane K. Winn, Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA, retrieved 9 July 2014, www.law.washington.edu..

20 Section 4 of the Act defines 'personal data' as to means any information in respect of commercial transactions, which—

(a) the General Principle;
(b) the Notice and Choice Principle;
(c) the Disclosure Principle;
(d) the Security Principle;
(e) the Retention Principle;
(f) the Data Integrity Principle; and
(g) the Access Principle[21]

From procedural law perspective, securing online evidence can be described as a method of acquiring or gathering evidence from online sources. In Malaysia, there is no specific court Rules or Practice Direction or cases that explain on methods to secure online evidences. However, inference can be drawn from cases related to discovery of documents according to the Rules of Court 2012. The Rules of Court 2012 provides several methods to gather or secure evidence or information. They include discovery and inspection of documents (O24), discovery by interrogatories (O26), Admission (O27) and Anton Piller Order. However, in this paper only Discovery and Inspection of documents and Anton Piller Order will be discussed since both methods involve production of documents.

DISCOVERY AN INSPECTION OF DOCUMENTS

The party may apply to the court for a discovery order under Order 24 Rules of Court 2012 (ROC). The court may allow the application and at any time order any party to a cause or matter to give discovery by making and serving fon any other party a list of documents which are of have been in his possession, custody or power and may also that person to make an affidavit verifying such a list. The list of documents must be in Form 38 and should contain two schedules, Schedule 1 and Schedule 2. Schedule I is divided into Part 1 and Part 2. Part I contains non privileged documents and Part 2 contains documents claimed to be privileged from production. Schedule 2 consists of documents which the party had, but does not now have, in his possession custody or power.[22] However, the court will not order for discovery method if it is not necessary. (O24). And sometimes, the party may challenge this procedure on the ground of privileged and privacy issues.

DOCUMENT AND ITS MEANING

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010;

[21] Section 5 of the PDPA
[22] White Book, *Malaysian Civil Procedure 2013*, Sweet & Maxwell Asia.

Document is defined as 'any matter expressed, described, or howsoever represented, upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, sound track or other device whatsoever,' by various means including by means of '(c) any sound recording, or any electronic, magnetic, mechanical or other recording whatsoever, and howsoever made, or any sounds, electronic impulses, or other data whatsoever' (section 3 of the Evidence Act 1950 (EA)(Malaysia). While the Penal Code defines document as 'a matter recorded, stored, processed, retrieved or produced by a computer.' (section 29(1) and (2) of the Penal Code (Malaysia). The first definition is wider that the second definition which specifically refers to matters done by the computer.

From the context of civil procedure, 'document' is 'anything in which information of any description is recorded and includes a claim, summons, application, judgment, order, affidavit, witness statement or any other document used in a Court proceeding'. (Order 1 rule 2 Rules of Court, 2012). In Malaysia, matters which have been held to be documents include tape recording, facsimile letter and the display on a video display unit as well as the printout of that video. [23] Other examples of documents include tape recordings of evidence or information (*Grand v Southwestern and County Properties Ltd* [1975] Ch 185]; microfilms which are used to keep records (*Barker v Wilson* [1980] 1 WLR 884 and a computer database which forms part of the business records of a company (*Derby & Co Ltd v Weldon* (No.9) [1991] 1 WLR 652; *Alliance & Leicester Building Society v Ghahremani* (1992) 32 RVR 198).

ANTON PILLER ORDER

This method is used to recover or secure incriminating evidence believed to be in the possession of the other party. It is used in cases such as piracy, counterfighting and infringement of intellectual property. The evidence for these cases may be available online and securing such evidence from the opposite party will require the applicant and his solicitors to enter and inspect the defendant's / repondent's premises and seize or copy any information relevant to the alleged infringing activities. However, the application for this Order is granted only if there is a real risk that the respondent would conceal or destroy relevance or incriminating evidence in his possession.[24]

Other than the above methods, digital investigation in cloud computing system can also be used in finding data or evidence in the cloud. This method requires good skills and knowledge and normally it is conducted by forensic expert who has to search for evidence from many sources whether inside or outside jurisdiction. [25]

ONLINE CIVIL CASES

The above methods can be used to secure online evidence in civil cases namely torts, contracts, land and trusts. Besides that, other laws such as the Evidence Act, Electronic

---

23 Augustine Paul, n.6 at p.16.

24 *Anton Piller v. Manufacturing Processes* [1976] Ch.55

25 Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir & Ors. A survey about impacts of cloud computing on digital forensics, *International Journal of Cyber- Security and Digital Forensics* (IJCSDF)2 (2): 77-94, 2013.

Commerce Act, Digital Signature Act, Defamation Act and Contracts Act are also relevant to be cited as referance. The followings are some of the cases:

CASE 1: ONLINE DEFAMATION

In filing a suit against another for defamatory words published online (either in facebook or twitter or other online sources), one must make sure that the evidence to establish the case still exists and securing such evidence will not affect the originality or authenticity of the evidence. In *Dato' Mohamad Salim Fateh bin Fateh Din* v *Nadeswaran a/l Rajah (No 1)*[26] the plaintiff, a prominent businessman, sued the defendant, a journalist, for publishing two defamatory statements about him on Twitter. In this case evidence of defamatory statement was downloaded from internet at http://twitter.com/CitizenNades while the second defamatory statement was downloaded from the defendant's twitter website. The two defamatory statements were posted on the defendant's twitter websites and have been seen by thousands of defendant's followers. Based on the facts, the court held that the defendant was liable for defamation. The court also granted the plaintiff's application for an injunction and awarded damages to the plaintiff.

CASE 2: ONLINE BREACH OF CONFIDENTIAL INFORMATION

This type of breach normally occurs when an employee transfers or uses the information or trade secret of his ex-employer to set up his own business. There are many cases where employees have been sued by their former employers due to breach of confidence. In *Ecooils Sdn Bhd* v *Raghunath Ramaiah Kandikeri*[27], the plaintiff's cause of action was premised on breach of the confidentiality clause or breach of confidence. The issue was not whether the information of the plaintiff's technology that was sought to be protected was unique or novel but whether it was a trade secret or confidential information. In this case, the plaintiff had proven on balance of probabilities that its technology of using SBE as fuel to produce energy and steam in a specially designed SBE Bio Mass Boiler was highly confidential information and a trade secret and that, in addition, it had trade secrets in the form of confidential information on the cost, benefits, pricing, cost-saving benefits, specific requirements of the specially designed SBE Bio Mass Boiler and the names of its SBE suppliers and customers. The defendant was employed in a capacity where such 'confidential' material was habitually handled. Thus, when the defendant had created and established a company ('KIS') it was clear that KIS was used as a vehicle to masquerade defendant's activities of disclosing and disseminating the plaintiff 's confidential technology, information or trade secrets to third parties whilst quietly establishing his business at the same time. The court allowed the plaintiff's claims.

Although the above case is not about online evidence the issue of confidentialilty is very important in employment contract. The employee may be sued based on the evidences such as email messages or other documents.

CASE 3: ONLINE BREACH OF CONTRACT OR BREACH OF E-CONTRACT

An electronic contract is an agreement created and "signed" in electronic form -- in other words, no paper or other hard copies are used.[28] Its position is similar to paper contract. This paperless contract is optional. (Section 3 of Electronic Commerce Act 2006) In the US, e-contract is optional since not all contracts are allowed to be concluded electronically. Further, in order to prevent abuse of electronic contract and to protect consumers certain documents

[26] [2012] 10 MLJ 203

[27] [2014] 7 MLJ 309

[28] Electronic signatures and online contracts. Retrieved 10 July 2014. http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html

are not valid and unenforceable in electronic versions. They include wills, codicils, testamentary trusts, documents relating to adoption, divorce, and other family law matters.[29] E-signature makes e-contract as valid as traditional paper contract. In fact, encrytion or electronic data encoding is an important tools in electronic contracts and communications. It ensures the confidentiality of electronic communications and data against the risk of theft, misuse, or alteration.[30]

Sometimes in business email and web are used to do business communication. The communication may include negotiation or agreement on certain clauses/ contractual terms. Are e-mails and web contracts enforceable? If the elements of a valid contract exist then such e-contract is valid and enforceable. If there is breach of e-contract, the lawyers may obtain or secure evidence by printing the emails or web contract and its prior email or web negotiations.[31]

CASE 4: INTERNET FRAUD

Internet fraud refers to fraud or online deceit. Fraud will still exist in ecommerce even though encryption technology is good enough to protect electronic transactions, but at least a good encryption technology can reduce fraud significantly.[32] Securing evidence from internet fraud may be quite easy but proving its commission or existance is very tough. In civil proceeding, fraud must be established by the plaintiff. According to Mohamad Ariff J in *Re Ng Liang Shing; ex parte Sirim Bhd* [2013] 8 MLJ 916, "the burden and standard of proof in civil proceedings in relation to fraud is a heavy one, and in this regard I am in full agreement with the lucid statement of the law by Vernon Ong J in *Mohd Nasir bin Moidu v Lee Swee Kim* [2011] 7 MLJ 606; [2010] 1 LNS 974, which I take the liberty to reproduce below:

> "In this case the onus is upon the plaintiff to establish the alleged fraud. The standard of proof is that of proof beyond reasonable doubt (*Boonsoom Boonyanit v Adorna Properties Sdn Bhd* [1997] 2 MLJ 62; [1997] 3 CLJ 17 (CA); *Narayanan Chettyar v Official Assignee,* Rangoon AIR 1941 PC 93, 95 applied in the Singapore High 920 Malayan Law Journal [2013] 8 MLJ Court in *Nederlandsche Handel-Maatschappij NV (Netherlands Trading Society) v Koh Kim Guan* [1959] 1 MLJ 173; [1959] 1 LNS 63; *Tai Lee Finance Co Sdn Bhd v Official Assignee&Ors* [1983] 1 MLJ 81; [1983] CLJ 387 (Rep); [1983] 1 CLJ 183; [1983] 1 MLJ 81 (FC); *Saminathan v Pappa* [1981] 1 MLJ 121; [1980] 1 LNS 174; *Chye Chew & Anor v Eastern Mining & Metals Co Ltd* [1965] 1 MLJ 201; [1964] 1 LNS 194 (FC) … Proof beyond reasonable doubt does not, however, mean proof beyond the shadow of doubt. The degree of proof must carry a high degree of probability so that on the evidence adduced the court believes its existence or a prudent man considers its existence probable in the circumstances of the particular case. If such proof extends only to a possibility but not in the least a probability, then it falls short of proving beyond reasonable doubt …"

The above decision implies that internet fraud requires very strict proof and should be beyond reasonable doubt or must at least a high degree of probability. In the above case, an appeal by JD was dismissed on the ground that the main evidence produced by JD was electronic evidence which the learned judge decided that" electronic or computer evidence, when admitted, also require to be tested against the normal rules on evidence on burden and standard of proof and the weight to be attached to the evidence. With respect, I find the relevance and weight to be given to the e mail trail and the electronic attendance record to

---

29 http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html

30 Kurt M. Saunders, Practical internet law for business, Artech House , INC: USA, 2001. At p27

31 Henry R. Cheeseman,The Legal environment of business and online commerce, sixth edition,2010, Prentice Hall: United States, p.200

32 Mohammad Nabil Almunawar, n.13.

fall far short of proof that the judgment debtor was actually in his department when the bankruptcy notice was purportedly served on him.".

PROVING AUTHENTICITY OF ONLINE EVIDENCE

Authenticity of online evidence is very crucial in order to establish one's case against the other. In order to preserve the online evidence digital encrytion techonology is used. This method will ensure that the evidence remains authentic and admissible. Usually, a forensic expert will testify that the evidence obtained is authentic and reliable. But, the counsel may argue on the reliability of expert opinion who is supposed to maintain the originality of the data collected.[33] The integrity of electronic messages is also emphasis in ECA 2006 (section 12). In civil cases, the lawyers have to proof authenticity of online evidence on the balance or probabilities except in internet fraud cases as mentioned above. The plaintiff must prove that the evidence is not modified or tampered with and it is authentic.

Since the court accepts only relevant documents the Evidence Act 1950 has laid down several provisions on the need to produce relevant documents. They are sections 6, 35 to38 and sections 90A to 90C. Although there are facts which need not be proof[34] proving reliability of evidence is essential. The court will also accept admissions and witness statements to prove the authenticity of the evidence. Thus, the witness must be able to identify the evidence and explain in court. The insertion of sections 90A, 90B and 90C to the EA 1950 affirm that evidence from computer is admissible if produced in compliance with the stated provisions. Although certificate is not needed to prove the evidence, the defence counsels can still rely on this defence. However, the issue of certificate was settled by the court in few decided cases.[35]

CONCLUSION

The above discussion shows that online evidence can still be secured and acquired by downloading and printing it. This form of evidence is more visible to the lawyers, investigators and the court. Email messages or statements in Twitter accounts are regarded as online evidences in few cases. Apart from DSA 1997 that auntenticate the online transactions, PDPA 2010 also provides protection to online data while the Evidence Act 1950 recognises the admissibility of online evidence. This is based on the word 'document' that includes computer output as evidence.In conclusion, when online evidence is printed the principle of documentary evidence will be applied and if it is relevant, authentic and reliable, such evidence shall be admissible as evidence.

REFERENCES

Almunawar, Mohammad Nabil. (July 2012).Securing electronic transactions to support e-commerce. Retrieved from http://arxiv.org/abs/1207.4292

Anton Piller v. *Manufacturing Processes* [1976] Ch.55

Alliance Management SA v *Pendleton Lane P and Another And Another Suit* [2008] SGHC 76,

---

33 Stephen Mason, Authentication of electronic evidence, Information Age, 18 October 2006 at http://www.ingfoage.idg.com.au retrieved on 10 May 2014.

34 Sections 56, 57 and 58 of the Evidence Act 1950.

35 The Singapore High Court decided that the computer evidence shall be admissible as long as the computer printout which was produced maintain its authenticity and accuracy as required by s35(1) (a) of the Singapore Evidence Act. See further *Alliance Management SA* v *Pendleton Lane P and Another And Another Suit* [2008] SGHC 76, [2008] 4 SLR 1.

[2008] 4 SLR 1

Business Dictionary. Retrieved from http://www.businessdictionary.com/definition/online.html.

Cheeseman, Henry R. (2010). *The Legal environment of business and online commerce*, sixth edition, United States: Prentice Hall, p.200

Chissick, Michael. (ed) & Kelman, Alistair. (2002). *E-commerce: Law and Practice,* 3rd edit, United Kingdom: A Thompson Company, Sweet & Maxwell Ltd. at 192.

Collins COBUILD English Dictionary. (1996) Scotland: HarperCollins

Daryabar, Farid., Dehghantanha, Ali., Udzir, Nur Izura., Mohd Sani, Nor Fazlinda., Shamsuddin, Solahuddin. & Norouzizadeh, Farhood. (2013). A survey about impacts of cloud computing on digital forensics, *International Journal of Cyber- Security and Digital Forensics* (IJCSDF)2 (2): 77-94

Electronic signatures and online contracts. Retrieved from http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html

Evidence Act 1950

Evidence Act (Chapter 97) (Revised 1997) (Singapore)

Kierkegaard, Sylvia Mercado. (Feb. 14, 2007). *E-Contract Formation: U.S. and EUPerspectives*, 3 Shidler *J. L. Com. & Tech.* 12 . Retrieved from http://www.lctjournal.washington.edu/Vol3/a012Kierkegaard.html

Mason, Stephen. (October 18, 2006). Authentication of electronic evidence, *Information Age*. Retrieved from http://www.ingfoage.idg.com.au

Mohd Ali Jaafar v Public Prosecutor [1998] 4 MLJ 210.

N Gopal, Oracle Database + 2 days: security Guide, 2011. Retrieved from docs.oracle.com/cd/B28359_01/server.111/b28337.pd

Paul, Augustine. (2004). *Evidence: Practice and Procedure*, second edition, Kuala Lumpur: Malayan Law Journal, at 17.

*Per*sonal Data Protection Act 2010

Public Prosecutor v *Dato' Seri Anwar bin Ibrahim (no 3*) [1999] 2 MLJ 1, 170 (HC)

R v *Turner* [1975] 1 All ER 60, at 74 (CA

Singleton, Susan. (1999). *Business, the Internet and the law*, Chapter 3, United Kingdom: Tolley's, at 65.

Saunders, Kurt M. (2001). *Practical internet law for business*, USA: Artech House, INC, p27

Top 10 ways to secure your stored data Retrieved from http://www.computerworld.com/s/article/9002188/Top_10_ways_to_secure_your_stored_data

White Book, *Malaysian Civil Procedure 2013*, Malaysia: Sweet & Maxwell Asia.

Wittie, Robert A. & Winn, Jane K. Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA. Retrieved from www.law.washington.edu..

http://www.dictionary.reference.com
http://www.nolo.com/legal-encyclopedia/electronic-signatures-online-contracts-29495.html
[2012] 10 MLJ 203
[2013] MLJU 252
[2014] 7 MLJ 309

AUTHOR'S BIOGRAPHY

Duryana bt Mohamed (Assistant Prof.Dr) is a lecturer at Ahmad Ibrahim Kuliyyah of Law, International Islamic University Malaysia. She graduated from the International Islamic University Malaysia in 1993 for her LLB (Hons) and in 1994 for her LLB (Hons) (Shariah). Later she obtained her Master in Corporate and Commercial Law from Queen Mary and Westfield College (QMW), University of London in 1995. She was called to the Malaysian Bar in 1997 and became an Advocate & Solicitor of the High Court of Malaya in 1997 (non-practising). She received her Ph.D in Civil Law from International Islamic University Malaysia (IIUM) in 2008 specialising on Electronic Evidence: Procedure and Admissibility issues. She teaches civil procedure at Ahmad Ibrahim Kuliyyah of Laws and have experienced teaching the Law of Contract, Law of Torts, Compulsory Moots and Cyberlaws at KICT, IIUM. Her area of specialization is in Electronic Evidence and Discovery of ESI but she is also interested in E-Commerce law and Cybercrimes. She can be contacted via email at mduryana@iium.edu.my