Gathering of Information in Internet Environment: Balancing the Right to Discovery and Right to Protect the Privacy under the Laws

Duryana Bt Mohamed

***Abstract*—Gathering of information in the internet environment is very challenging since the information may be available at different places. There are many methods to gather information and one of it is by way of discovery of document. This discovery process is adopted when preparing one's case for a full trial. It is used to gather information which is not adequate and the party needs to get relevant documents from the opposite party as to complete his case. The opposite party in the suits may be an individual, company, government agency or its servant. When the court order for discovery the opposite party is expected to comply with it but in some cases, the opposite party refuses to do so citing privacy issue as his or their reason for refusal. The issues are how to effectively implement discovery against them and how to balance between the right to discovery and right to protect the privacy of their clients. What is actually their liability towards the plaintiff and what are the consequences of failure to comply with discovery order. This paper will discuss and analyse the above issues by presenting laws and court decisions pertaining to discovery of documents as practiced in Malaysia and several other countries.**

***Index Terms*—Court decisions, discovery right, internet, privacy right, the laws,**

I. Introduction

Internet environment is borderless in nature. This means the information is available at various places and in various formats. But under the laws, there are several methods that one can use to gather information from the internet. One of the methods is by way of discovery of document or information. This discovery process is adopted during the pre trial stage and it is used to gather information which is relevant to the case. Through discovery process the parties will be able to gather all relevant documents to prepare and complete their case before the case is being heard. The opposite party in the suits may be an individual, company, government agency or its servant. Practically, when the court order for discovery the opposite party is expected to comply with it but in some cases, the opposite party refuses to do so citing privacy issue as his or their reason for refusal.

The issues are how to effectively implement discovery against the opposite party and how to balance between the right to discovery and right to protect the privacy of his or their clients. What is actually their liability towards the plaintiff and what are the consequences of failure to comply with discovery order. This paper will discuss and analyse the above issues by presenting laws and court decisions pertaining to discovery of documents that contain relevant information as practiced in Malaysia and several other countries.

Manuscript received September 5, 2012; revised January 16, 2013. This work was supported in part by Research Management Centre of the IIUM under Grant Type B (Endowment).

Duryana Mohamed is with the Legal Practice Department, Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia (IIUM) (e-mail: mduryana@iium.edu.my).

II. Implementing Discovery

A. Discovery as Method of Gathering Information

Discovery is one of the methods to gather relevant documents or relevant information before the trial. According to Malaysia Rules of Court 2012 (RC) '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) while the UK Civil Procedure Rules 1998 (CPR) defines 'document' as 'anything in which information of any description is recorded' (Part 31.4). The Oxford Dictionary defines 'information' as 'facts provided or learned about something or someone or what is conveyed or represented by a particular arrangement or sequence of things or genetically transmitted information which also includes data processed, stored, or transmitted by a computer'[1].

The above method has been adopted by the English court since the Nineteenth Century by the English equity procedures. Previously, in England this process was governed by the Rules of Supreme Court 1965 (RSC). Then, the process was governed by the Civil Procedure Rules 1995 which later amended and presently known as Civil Procedure Rules 1998. This rule came into effect in 1999. Other than the UK, discovery is also adopted and applied in countries like the United States (US), Malaysia, Australia and Singapore.

B. Discovery under the Law

Discovery of documents is discussed under the civil procedure law of most common law countries. This method is useful when parties need to gather documents that contain information related to civil suits or cases. The civil suits may include cases of breach of contracts, breach of duty of care or negligence, breach of trusts, copyright infringement and trademarks. When technology develops and the use of electronic documents (e-documents) arises this method is given further attention especially by the lawyers. The reason behind this is because the information is now available in various electronic formats which require the application of electronic discovery in gathering those e-documents. Further,

in Internet environment discovery is not limited to paper documents only but extends to discovery of information or online social networks such as Facebook or Myspace [2].

In the US, the discovery procedure is provided by Rule 34 of the US Federal Rule of Civil Procedure (F.R.C.P). This rule was reviewed and amended in 2006 as to provide more clear provision on electronic discovery (e-discovery). Among the affected and updated rules are Rules 16, 26 and 34 which deal specifically with e-discovery procedures. Meanwhile Rule 37 deals with Sanctions and Rule 26 provides for general provisions governing Discovery and Duty of Disclosure. After 2006, the FRCP seems to be the most updated and extensive civil procedure rules on e-discovery as compared to other countries.

While in the UK discovery is known as 'disclosure'. The reform made to UK Civil Procedure Rule in 1995 has resulted with new UK Civil Procedure Rule 1998 (CPR) [3]. This Rule came into force on 26th April 1999. E-discovery is provided by Part 31 of UK CPR 1998. According to Part 31.1 of the same rule, 'disclosure' happens when 'a party discloses a document by stating that the document exists or has existed'.In New South Wales (NSW), Australia discovery of documents is provided by Part 23, rules 3 and 4 of the Supreme Court Rules 1970 (SCR). The Supreme Court of New South Wales has introduced a limited discovery regime under which parties may apply for an order for discovery of documents within a class or classes specified in the order and for discovery of one or more of documents within a class (Part 23, rule 3 (1) of the SCR 1970). The rules also provide that a class of documents shall not be specified in more general terms than the court considers to be justified in the circumstances (Part 23 r 3(2) and r3 (3) of the SCR 1970) [4].Other than the SCR there are also other civil procedure rules in different territories in Australia such as Uniform Civil Procedure Rules 2005 (NSW) and Uniform Civil Procedure Rules 1999 (Queensland).

In Singapore and Malaysia, discovery process is provided by Order 24 of Singapore Rules of Court 1996 (RC) and Order 24 of the Malaysian Rules of Court 2012(RC), respectively. The two Rules are quite similar when Malaysia adopted the new RC since August 2012. These rules provide among others that discovery is only ordered by the court when it is necessary and parties who applied for discovery order must first establish that the documents requested are in the possession, custody and power of the other party. There are also certain court forms provided by Order 24 of RC 2012 which the parties are required to complete when using this method. The forms are Form 38 (List of Documents), Form 39 (Affidavit verifying List of Documents), Form 40 (Notice to Inspect Documents), Form 41 (Notice to produce documents referred to in pleading or Affidavits) and Form 42 (Notice where documents may be inspected). If the party so ordered objects to produce any documents or offers to inspect the documents at an unreasonable time or place, the Court may on the application and affidavit of the party entitled to inspect the documents make an Order in Form 43 (Order for production of documents and inspection) against the other party.

The Rules on discovery in the US, UK, Australia and Singapore have been tested in cases involving electronic discovery. These can be seen in court decisions relating to discovery of electronic data in the above countries. In the US alone there is a data base on 1500 cases of e-discovery compiled by K & L Gates. The cases were compiled according to their categories. The categories include e-discovery rules, context and particular issues. This data base shows that e-discovery method is growing and becoming popular among the US litigators [5]. However, in Malaysia the situation is very much different. Order 24 has not been tested on e-discovery cases and very few lawyers are aware of e-discovery. Nevertheless, it is hoped that with the changing of the laws and updates on e-discovery practices Malaysian lawyers will finally use this method in the future [6].

Although there is a compilation of cases on discovery and a growing interest on e-discovery the issues are how to balance the right to discovery of documents and the right to protect the privacy. What are the arguments raised by the parties in maintaining their rights? These issues will be discussed below.

III. Balancing the Right to Discovery and Right to Protect the Privacy

In every discovery request there should be a balance between the right to discovery of documents and the right by the other party to protect the documents requested. The protection is needed since there may be elements of privacy in the documents and disclosing those documents will affect the other party's reputation or other businesses.

For companies, once they involve in litigation they must quickly review their stores. The electronically stored information or ESI will then be identified and classified into their relevancy, privileged and non –privileged status. At this stage, the companies are required to protect and preserve relevant ESI when the law suit or investigation is anticipated.

A. Right to Discovery under the Law

Who have the right to apply for discovery of documents and request for information? When the right to discovery accrues? The answer to the first question is that any party to any civil cases may apply for discovery if he thinks that there is still an incomplete information or evidence to prepare his case. The right to discovery accrues or begins when the court make an order for discovery under Order 24 rule 3 or rule 7 of the RC 2012. The documents which may be ordered to discover are provided by Order 24 rule 3 (4) of the RC 2012. They are as follows:

"a) The documents on which the party relies or will rely; and

b) The documents which could:

1) Adversely affect his own case;
2) Adversely affect another party's case; or
3) Support another party's case."

Order 24 rule 7 provides that the Court may make order for discovery of particular documents. But this order is made only after an application for discovery of particular documents is made by any of the parties. The application must state that the documents requested are within the possession, custody and power of the other party. The Court

will grant the application only after it satisfies with the grounds of the application provided by the applicant. Rule 8A of Order 24 further provides that the party required to give discovery under Order 24 rule 3 or 7 'shall remain under a duty to continue to give discovery of all documents falling within the ambit of such order until the proceedings in which the order was made are concluded'.

Discovery can also be made against other person before or after the commencement of the proceedings. (Order 24 rule 7A). If it is made before the commencement of the proceedings then originating summons (OS) shall be used but if it is made after the commencement of the proceedings a person who is not a party to the proceedings shall make the application by using a notice of application (NA). Both the OS and the NA shall be supported by an affidavit. Nevertheless, the Court may reject the application for discovery if it is amount to fishing expedition or irrelevant request.

Is accurate discovery request necessary? In the US case of Mosaid Technologies Incorporated v. Samsung Electronic Co., Ltd., Samsung Electronics America, INC., Samsung Semiconductor, INC., and Samsung Austin Semiconductor [7] the plaintiff requested production of a document, but did not specify accurately the type of document. The other party argued that the plaintiff must make a specific request for the e-mail. The court found that *Samsung*'s argument was wrong on the ground that, although *Mosaid* did not use the word 'e-mail' in its discovery request, it broadly defined the word 'document' to include, without limitation, 'type…matter,' 'other data compilations,' 'letters', 'correspondence,' 'notes to the files,' 'interoffice communications,' and 'statements'. Thus, this case suggests that a specific request using the term e-mail is not necessary because an 'e-mail' is considered as a 'document' and it falls within the scope of the US law on discovery of documents.

But it is still important to accurately name the documents requested. This is because an accurate discovery request is important because it will help in narrowing down the scope of the investigation by focusing on obtaining information from specific sources in specific locations [8].

Then, subject to the court discretion either to grant or not to grant the application or discovery request. If the court thinks that the discovery is necessary the court would make discovery order against the other party.

B. Right to Protect the Privacy under the Law

When the other party receives the court order for discovery he is expected to comply with such order. But he may argue that the documents needed are not relevant, not in his possession and they are privileged document. Therefore, disclosing such documents would amount to violation of their clients' privacy and confidential information. In this regard, parties may argue their case based on the relevant laws on protection of personal data or information such as the Personal Data Protection Act 2010 (Malaysia) (PDPA), Stored Communication Act 1986 (SCA) (US), Copyright Act 1997 (Malaysia), Data Protection Act 1998 (DPA) (UK), Freedom of Information Act 2000 (FIA)(UK), the Electronic Transactions and Commerce Law No.2/2002 (Dubai) (ETCL), the UAE Federal Law 2 of 2006 on the Prevention of Information Technology Crimes (PITC law) the UAE Constitution and the UAE Penal Code. In fact, there are many other relevant laws on data privacy. However, this part will only discuss the application of these laws in Malaysia, Australia and the US.

In Malaysia, the law on protecting privacy and personal data protection has come into force in January 2013. But the public or the consumers are expected to take control of their own personal data [9]. This means, this Act will only be effective if the consumers know their rights and limitations. Prior to the enforcement of this law the companies and organisations have used the personal data or information of their customers to promote their products. But beginning January 2013, activities like telemarketing or solicited emailing messages to any addresses which the companies bought from a third party are not allowed or rather restricted. Nevertheless, the public still need to disclose their personal data if they are required to do so by the Government authorities and Government-link companies. This is one of the exemptions in the PDPA. Hence for security reason, the public should know their rights and lodge complaint to the relevant authority immediately after knowing that the data users (companies/organisations) have misused their personal data.

In Australia, the privacy issues are governed by the Privacy Act 1988 (Cth). This Privacy Act imposes significant restrictions on the ways in which organisations can deal with personal information they have collected about individuals, and is also one of the tools consumers can use if they feel an organisation has mistreated them, or inappropriately dealt with or disclosed their personal information[10]. In May 2012, the Attorney General office for Australia has announced that the Australia's privacy laws will be reformed to better protect people's personal information, simplify credit reporting arrangements and give new enforcement powers to the Privacy Commissioner. Attorney-General Nicola Roxon said, "In an increasingly digital world, both consumers and governments have a role to play to protect privacy. In introducing these changes, the Gillard Government is doing its bit to protect the privacy of Australian families." This reform will benefit mostly the consumer in Australia [11].

While in US, there are a number of federal and state laws on privacy. There is also an International Privacy Laws. Among the US data privacy laws are Electronic Communications Privacy Act 1986 (ECPA), Electronic Freedom of Information Act 1996 (E-FOIA), Privacy Protection Act 1980 and Stored Communications Act (SCA). The SCA protects communications stored by two different types of online services: electronic communication service ("ECS") providers and remote computing service ("RCS") providers. Further, the Act only applies to communications stored on the Internet by third-party providers. This means an individual cannot use the SCA to avoid a court order requiring her to disclose online information herself. In *Reid* v *Ingerman Smith LLP* [12] the US court ruled that privacy alone does not justify shielding information from discovery. The court cited the example of personal diaries, which are discoverable if they contain relevant information regarding contemporaneous mental states and impressions of

parties. Further, the appropriate scope of discovery, according to the court, includes social media communications and photographs "that reveal, refer, or relate to any emotion, feeling, or mental state . . . [and] that reveal, refer, or relate to events that could reasonably expected to produce a significant emotion, feeling, or mental state."

As regard to discovery of privileged documents this discovery could be avoided if the parties or their counsel have knowledge about their information technology (IT) system and also understand the duty to protect privileged information under the law. According to section 126 of the Evidence Act 1950 (Malaysia);

"No advocate shall at any time be permitted, unless with his client's express consent, to disclose any communication made to him in the course and for the purpose of his employment as such advocate by or on behalf of his client, or to state the contents or condition of any document with which he has become acquainted in the course and for the purpose of his professional employment, or to disclose any advice given by him to his client in the course and for the purpose of such employment".

The above section emphasises on the duty of the counsels to protect their client's privacy and privileged information. However, if the plaintiff had mistakenly disclosed privileged documents he cannot then make a claim to recover all the documents previously disclosed to the defendants. In this regard, Vinelott J in Derby & Co. Ltd v Weldon & Others (No10) [13] stated that the plaintiffs could not claim privilege in relation to the tape recording or the transcripts which had been inadvertently disclosed in the course of discovery. He further added that the defendants were entitled to assume that the documents included by the plaintiffs were documents which they proposed to rely on whether privilege or not. (See page 923)

The above mentioned argument was used by parties who usually involved in cases of copyright infringement. While in cases of medical negligence, the Court of Appeal in Malaysia has also decided that opinions of medical reports obtained by the plaintiff are the subject of legal professional privilege and hence protected from pre-trial discovery under Order 24 of the previous Rules of the High Court 1980 and the present RC. This judgment was made in Dr Pritam Singh v Yap Hong Choon [14].

In addition to that, if the documents are categorised as ESI then the companies are supposed to have their discovery policy and e-discovery best practices rule to conduct proper discovery of ESI or e-discovery. These two policies will ensure that the process of e-discovery is easier to be conducted.

IV. Liability to Disclose

When order for discovery is made by the court the party receiving such order is expected to obey the order and allow for discovery. Such discovery or disclosure is considered as liability of the defendant towards the plaintiff or the claimant. However, this liability depends on the circumstances of the case. The defendant may refuse to disclose documents requested on the ground of privacy or privileged information as mentioned above. The other ground is that the said documents are not in his possession and they are not relevant to the case. Hence, it is important to balance the right for discovery on the part of the plaintiff and right to protect the privacy on the part of the defendant. Cases have shown that this balance of right is achievable if parties know their rights and obligations in civil litigation.

Although, in cases of copyright infringement or internet defamation the defendant (the Internet service provider or any companies or individuals) would usually argue that they are not liable for such infringement or defamatory statements this argument should not deter the court to enforce the right of any of the parties. Incidents such as deleting information, delaying to disclose or refusing to disclose the documents requested are common but court has discretion to decide in whose favour a judgment should be granted.

V. Consequences

Previously, Order 24 of the Rules of the High Court 1980 (RHC) provides that a party shall be liable to committal for failure to comply with discovery order. However, after the amendment in 2012, Order 24 of the RC 2012 provides no punishment for such misconduct. Instead, under sub-rule (5) to rule 16 of Order 24 RC, the party may not rely on those documents except with the leave of the court. The same rule also provides that if the party so ordered fails to comply with discovery order or fails to produce any documents for inspection the Court may order that the action be dismissed or order the defence to be struck out and judgment to be entered accordingly. In Perbadanan Nasional Berhad v. Syed Omar Syed Mohamed, the court ordered the case to be struck out because there was a failure to comply with discovery order by one of the parties [15].

In the US sanctions will be imposed on failure to comply with discovery order. This can be seen in *Furminator, Inc*.v *Petvac Group LLC* [16] where the district court granted sanctions for repeated discovery misconduct by the defendant. The defendant in this case has willfully violated court orders on multiple occasions such as consistent refusal to abide by the docket control and discovery orders and also failing to timely answer the complaint. While in *DL* v *District of Columbia* the Chief Judge imposed privilege waiver sanctions against the defendant for repeated discovery misconduct. The misconducts or violations included failure to timely produce documents, violation of multiple discovery orders, failure to timely provide a privileged log and failure to inform the court of any delays in production in order to request appropriate extensions [17]. In *Carrillo* v. *Schneider Logistics, Inc.*, the US court had ordered monetary sanctions on the defendant who failed to comply with its discovery obligations i.e. by (1) failing to conduct a reasonably diligent search, (2) improperly withholding responsive documents, and (3) failing to take adequate steps to ensure preservation [18].

The Challenges

There are many challenges in gathering information from internet environment. One of them is difficulties in finding the exact place of where the data is located. This is because data is stored, located, saved and protected using different

systems and programming. Some documents are even created in many different languages, often on custom applications localised to a specific area of the world [19]. Sometimes, data may also be deleted and tampered by unauthorised user or even the owner of the data.

As for discovery process, the challenge faced by the party is to ensure that documents to be discovered as listed in the List of Documents (Form 38) fulfill the requirements of discovery. The documents must not contain privileged information that may lead to data breaches or any violation of privacy of the other party. If there is any such breach the party who is supposed to allow discovery and inspection of documents may refuse and raise objection. In this situation, the lawyers defending the party must be able to establish that the documents or information are confidential and they are privileged documents.

Other than that, implementing best discovery practices is also challenging since the company needs to maintain consistency, cost and communication. Consistency is required in implementing best practices and discovery policies at various locations for various time frames and results are predictable. There must also be consistency in communication among companies, attorneys and vendors [20].

However, managing cost of discovery is the most challenging. According to Kelly, cost of collecting potentially relevant document in electronic format or ESI have ballooned as ESI has grown more voluminous, taken more forms, and become scattered through thousands of different sources. For example, potentially relevant ESI might be contained in Word documents, Excel spreadsheets, PDFs, TIFFs, emails, instant messages, voicemail WAV files, or in any number of other formats, and might be located on an employee's personal computer or PDA, a server, a backup tape, a database, or any number of other sources [21].

For lawyers, they are expected to be more techno savvy. Since the next phase of internet or Internet of Things (IoT) and cloud computing are already taking place and adopted by the industries and businesses the lawyers should be prepared to face more challenges in the future. It is advisable for lawyers in Malaysia and some other countries to adopt e-discovery method in their practice since in the US there are already groups of e-discovery attorneys who focus on e-discovery and its related cases only [22].

For the effective implementation of e-discovery, the parties in the action should discuss and agree on the extent of reasonable search for documents. This act will limit the scope of discovery and its process.

VI. Conclusion

Internet environment provides opportunities to the people to create and store their information electronically. This online information is useful when disputes arise. Therefore, it is necessary to have a proper record of information and data. The information should be protected when there is an attempt to breach the online privacy. Discovery of information is one of the methods to gather information from the Internet. But this process will be quite complicated when the documents or information to be gathered involve privileged information and privacy issues. This explains why balancing the right to discovery and right to privacy is very important. Although there are several laws governing discovery and privacy the procedures and available protection may differ from one country to another. Certain countries are even struggling on implementing e-discovery and its best practices. This includes Malaysia where legal practitioners are still not prepared to adopt this method. Among the reasons are unawareness, lack of regulatory frameworks and the high cost of discovery. Hence, in order to be successful in gathering of information from the internet and to implement e-discovery all parties should give cooperation by complying with the court order for discovery and be reasonable in arguing on the right to protect privacy.

Acknowledgment

Thank you to my research assistant for helping me in finding the materials for this research project.

References

[1] See the Rules of Court 2012. [Online]. Available: http://www.kehakiman.gov.my and the meaning of 'information', [Online]. Available: http://oxforddictionaries.com/definition/english/information?q=information.

[2] A. W. Ryan, "Discovering facebook: Social Network Subpoenas and The Stored Communication Act," *Harvard Journal of Law and Technology*, vol. 24, no. 2, Spring 2011.

[3] Civil Procedure Rules 1998 (CPR). [Online]. Available: http://www.opsi.gov.uk/si/si1998/19983132.htm.

[4] S. Lindsay and C. Geoffrey. *Guide to the Practice of the Supreme Court of New South Wales*, U.K. : The Law Book Co. Ltd., 1989, at pp. 86-92 and Cairns, Bernard C., *The law of discovery in Australia: Documents, interrogatories and property*, ch. 2, 'Civil Litigation Practice and Procedure', (ALRC IP 20, 7). [Online]. Available: http://www.austrli.org/au/other/alrc/publications/issues/20/07cicill.html. See also *BT (Australasia) Pty Ltd* v *State of New South Wales & Anor* (No 9) (No 7) (1998) 153 Law Review (LR) 722 and *Roger Stafford Atkinson & Ors* v *State of New South Wales*, New South Wales Supreme Court (NSWSC) , pp. 400, 2005.

[5] Searchable e-Discovery Case Log. [Online]. Available: https://extranet1.klgates.com/ediscovery/.

[6] S. Sivanathan. (February 8, 2012). E-discovery: Changing the rule of the game. [Online]. Available: http://www.cyberintelligence.my/?p=360.

[7] See 18 U.S.C. § 2703.

[8] M. Devin, Electronic commerce in the 21st century: Article the discovery of electronic data in litigation: what practitioners and their clients need to know, William Mitchell Law Review (Wm. Mitchell L. Rev), no. 27, 2001 at 1825 and Cohen, Adam I. *E-discovery: Law and Practice*, U.S.: Aspen Law Publisher, ch. 10, 2004.

[9] H. Azizan. (4 January, 2013). Consumers, take control of your personal data [online] Available: http://thestar.com.my/news/story.asp?file=/2013/1/6/nation/.

[10] W. Emma, R. Cullough, and P. Rules, "The Increasing need for Organisations to Comply with Privacy Laws," *Legal Network Series (LNS(A))*, vol. 1, 2010

[11] Privacy laws set to reform. [Online]. Available: http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Second%20Quarter/2-May-2012---Privacy-laws-set-to-reform.aspx.

[12] *Reid* v *Ingerman Smith LLP* 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012). [Online] Available: http://www.legaltxts.com/2013/01/ and http://op.bna.com/eg.nsf/id/pdon-93escw/$File/reid1212.pdf.

[13] Derby & Co. Ltd v Weldon & Others (No10), Weekly Law Report (WLR), vol. 1, pp. 660, 1991.

[14] P. Singh and Y. H. Choon, *Malayan Law Journal* (MLJ), vol. 1, pp. 31, 2007.

[15] P. N. Berhad and S. O. S. Mohamed, *Legal Network Series* (LNS). vol. 1, pp. 96, 2011.

[16] Case No. 2-08-cv-338-TJW (E.D.Tex. Aug 5, 2011).

[17] D. E. Backhouse. Chief Judge Imposes Privilege Waiver Sanctions against Defendant for repeated Discovery Misconduct in *DL v District of Columbia*, the National Law Review. [Online]. Available: http://www.natlawreview.com. See also Mohamed, Duryana, "Discovery of electronically stored information (ESI) or e-discovery: The law and practice in Malaysia and other jurisdictions," in *IEEE Proceedings on the International Conference of Information Society (i-society)*, London, pp. 461-465, June 25-28, 2012.
[18] No. CV 11-8557-CAS (DTBx), 2012 WL 4791614 (C.D. Cal. Oct. 5, 2012).
[19] B. Matthew. (4 May 2006). Law in business: Language barriers, Legal Week. [Online]. Available: https://www.lexisnexis.com/ap/auth/
[20] A. James, "Implementing Effective E-Discovery Programs," in *E-discovery Best Practices*, United States: Aspatore, pp. 99-114, 2008.
[21] F. Kelly, "Reducing civil litigation costs by promoting technological innovation: Adopting standard of reasonableness in e-discovery," *Hastings Law Journal*, vol. 63, pp. 1167-1175, May 2012.
[22] Our Attorneys. E-Discovery Law. [Online]. Available: http://www.ediscoverylaw.com/promo/our-attorneys

Duryana Bt Mohamed was born in Malaysia on 31st of December. The author obtained her first degree in Law or LLB (Hons) from the IIUM, Malaysia; a second degree in Syariah Law or LLB (Shariah) (Hons) also at IIUM. Then she continued doing her Master of Laws (LLM) at Queen Mary & Westfield College, University of London and later obtained her PhD in Civil Law from IIUM, Malaysia. She has been working with IIUM since 1993 as a Tutor then promoted to the post of Assistant Professor Dr. in 2008. She is now a LECTURER at Department of Legal Practice, Ahmad Ibrahim Kuliyyah of Laws and teaching Civil Procedure law as her main subject. Other subjects that have been assigned to her in the previous years include the Law of Contract, The Law of Torts, Cyberlaw and Compulsory Moots. Since 2010 she has published few articles in national and International Journal. Among the articles are 'Computer Evidence: Issues and the Challenges in the Present and in the Future' and 'The process of gathering evidence in civil cases: Its application in civil and syariah court'. A chapter on 'E-commerce and the Practice in Malaysia' was also published in 'Law and Commerce: The Malaysian Perspective in 2011. Currently, she is completing research three projects namely, on e-discovery, child evidence and regulating blog business together with her colleagues from the same university. The last two projects are sponsored by Ministry of Higher Education (MOHE).