Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2018 = 6.371, www.srjis.com
PEER REVIEWED JOURNAL, MAR-APR, 2019, VOL- 6/50

THE CHALLENGES ON ENFORCEABILITY OF ONLINE CONTRACT

Prativa Panda[1], Ph. D. & Gagan Kumar Mallick[2]

[1]*Associate Professor, University Law College, Utkal University*

[2]*Research Scholar, P.G. Dept of Law Utkal University*

Abstract

With the development of era and the globalization, E-Commerce is an emerging factor for trading world. Online contracts are the contracts which take place through e-commerce, without meeting of the parties to the contract. These contracts are generally very similar to the paper based commercial contracts in which the commercial transactions conducted and concluded electronically through internet.Nevertheless, not all principles of contracts will or can apply in the same manner that they apply in traditional paper-based and oral contracts. But it is a contract of utmost good faith.In India,the recognition of an electronic contract is mainly supported by the Information Technology Act; 2000.The evidentiary value of E-contract has been well explainedin Indian Evidence Act. Sections 85A 85B, 88A, 90A and 85C of Evidence Act deals with presumptions as to electronic records whereas section 65B relates to the admissibility of electronic records. The e-contracts have their own merits and demerits. On the one hand it reduce costs, saves time, fasten customer response and improve servicequality by reducing paper work, thus increasing automation. However, many aspects of an online Contract, in particular, the requirements of signature and stamping, remain uncertain and confused. Although, many advantages offered by the information technology, a number of challenges have been also posed on the existing legal system. The researcher will make an attempt to analyse the various challenges and legal issues in this paper

***Keywords**: E-commerce, E-contract, IT Act2000 and Indian Evidence Act.*

INTRODUCTION:

The Internet has revolutionized people's way of communicating. In addition, the way people are doing business has also changed the Internet and electronic data exchange. It created a new kind of trade and trade called e-commerce. In an electronic world e-commerce brought about a new form of contract. The most common form of E-contracts is "End User License Agreement" or the EULA where the installation of software or terms/conditions/ user agreement on the Website requires a click on the" I agree" button.

Types of E-Contracts

1. Browse Wrap Agreements:

[1]***Associate Professor, University Law College, Utkal University***
[2]***Research Scholar, P.G.Dept of Law Utkal University***

This agreement is considered as a browse wrap agreement which is intended to be binding upon the contracting party by the use of the website. These include the user policies and terms of service of websites such as Flipkart or E-bay.

2. Shrink Wrap Contracts:

It is derived from the name 'shrink-wrap' packaging that generally contains the CD Rom of Software. The terms and conditions of accessing the particular software are printed on the shrink-wrap cover of the CD and the purchaser after going through the same tear the cover to access the CD Rom.When the CD is loaded to the computer some additional terms are also imposed in such license which appears on the screen only. If the new terms are not suitable to him the user has the option of returning the software.

3. Click or web-wrap agreements:

Click-wrap contracts are web-based contracts that require the user's consent or consent through the "I Accept," or "OK" button. The user must accept the terms of use of the particular software with the clickwrap agreements. Users who disagree with the terms and conditions cannot use or purchase the product after cancellation or refusal. Someone almost regularly observes web-wrap agreements. The terms of use shall be set down before acceptance by the users.

4. Electronic Data Interchange (EDI):

These are the contracts which are used in trade transactions enabling thetransfer of data from one computer to another in such a way that eachtransaction in the trading cycle can be processed with virtually no paperwork. Here unlike the other two there is exchange of information andcompletion of contracts between two computers and not an individual and acomputer.

Formation of Online Contract:

An e-contract is very different from a traditionalcontract. It can be created by exchanging email communication or by website forms.A contract would also be valid for the terms of use of a website once the user accepts the contract by clicking "I Agree."The End User License Agreement (EULA) also forms valid contracts in which end users click "I Accept" or "I Accept the Terms."

Laws Governing E-Contracts in India:

It is a revolution which modified contracts into e-contract. But it poses a lot of challenges and legal issues which need to be taken intoconsideration.

1. Indian Contract Act1872:

Every contract which are made and performed in India must be comply with the provisions of Contract act to make it legally enforceable. Where electronic record is used in the formation of contract that shall not be denied the validity or enforceability on the sole ground that data messages are used for that purpose. As between the originator and the addressee of the electronic record, a declaration of will or other statements should be valid, effective or enforceable even though it is in the form of database.

2. Information Technology Act, 2000:

Section 10A of the Information Technology Amendment Act, 2008" clearly states that the "Validity ofcontracts through electronic means, that "Where in a contract formation, the communication of proposals, the acceptanceof proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by meansof an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronicform or means was used for that purpose. "The Act also lays down the instruments to which the Information TechnologyAct,2000 does not apply, to negotiable instruments, power of attorney, a trust deed, a will, and contracts for sale ortransfer of Immovable Property.

3. Indian Evidence Act:

Now-a-days, the digital voicerecorder, digital cameras, digital video cameras, video conferencing are adding a new dimension to the evidentiary regime.The emergence of information and communication witnessed a sea change by elevating the status of the evidence recorded,generated or stored electronically from the secondary to primary evidential status. The evidentiary value of e-contracts canbe well understood in the light of the various sections of Indian Evidence Act.Sections 85A, 85B, 88A, 90A and 85C dealwith the presumptions as to electronic records, whereas, Section 65B relates to the admissibility of the electronic record.

Study of Case Laws:

In *Harpalsinghchotavs State of Punjab*[3] the supreme Court have reiterated the case that any electronic record in form of secondary Evidence cannot be admitted as Evidence unless a certificate of evidence under the section 65B of Indian Evidence Act

In *Hyderabad E-tender plan hacking case*[4] hackers havehacked the entire E- tender plans and allegedly charged RS.15000 pertender information to the government of Telangana.

In *Anwar Basheervsp.k.Basheer*[5]SupremeCourt hasrevised the law on electronic evidence. TheJudgement will have an impact on the manner in which wiretapes arebrought before the court

In *Casio India Co.Ltdvsashitateleservices Pvt LTD*[6] the Delhi high court held that once the website is accessed inDelhi it is enough to involve the territorial jurisdiction.

In Mehta *v. pereirafernandes*[7]therewas an appeal against a district court judgement which awarded the plaintiff company with the sum of 25000 euro. The amount was awarded allegedly from the amount arose from the email send by theMehta's solicitor

Security aspects with respect to Online Contracts:

The three major concerns for international electronic contracting are ***authenticity, enforceability and confidentiality.***Authenticity involves the verification of the person that one is dealing with electronically. Enforceability includes the legal scope of the license granted or the warranty given under a national law. It also includes the provability and verification of the contractual terms of an online transaction. Confidentiality revolves round the protection of sensitive information such as payment information and trade secrets. The fear is that the public domain nature of e-commerce makes such information, susceptible to fraud and misappropriation by third parties. The minimum level of due diligence pertaining to these three concerns entails a workable knowledge of the legal requirements of forming and proving a contract formed through the internet.

ISSUES AND CHALLENGES:

1.*Capacity to contract:*

[3]2014
[4]2016
[5]AIR 2014 SCW 5695
[6]AIR 2006 SC 730
[7] {2006] EWHC 813 (Ch)

Service provider has no idea whether the individual who has clicked on "IAgree" text or icon is legally competent to enter into a contract, whichaccording the Indian Contract Act, 1872, is one of the pre-requisites of avalid contract [sections 10, 11 & 12]. Contracts entered into by individuals, who are not competent to contract are void.

2. Electronic Authentication or Digital signature:

Online medium electronic authentication has to be done by "electronic records and digital signatures". Electronic records needs to be validated under the rules of evidence and procedure. The Information Technology Act, 2000 provides for the use of digital signatures to authenticate electronic records. Section 3 of the Act provides the whole process of digital signature creation and its verification which is based on UNCITRAL'sModel Law on E-commerce. A digital signature is the term used for marking or signing an electronic document, by a process meant to be analogous to paper signatures, but which makes use of a technology known **as public-key cryptography**. Additional security properties are required of signatures in the electronic world. This is because the probability of disputes rises dramatically for electronic transactions without face-to-face meetings, and in the presence of potentially undetectable modifications to electronic documents. Digital signatures address both of these concerns, and offer far more inherent security than paper signatures. Compared to all other forms of signatures, digital signatures are by far the most easily verified and the most reliable with respect to providing document integrity.

The Process of Creating a Digital Signature is very costly which cannot be affordable to everyone.

3. Jurisdiction of court:

The problem arises, if he is a non-resident, what laws would be applicable – domestic laws of the state where he is residing or domestic laws of the state whose laws he has committed the offence. In an online medium, fixing the choice of law becomes a more complex problem.

4. Indian Stamping laws:

The most difficult hurdle to be crossed by corporate India while executing a commercial contract electronicallyiscompliance with *Indian Stamping laws*. The Indian Law stipulates that any instrument chargeable wit duty (including electronic document) must be stamped in accordance with the relevant laws, immaterial of the form of execution. Appropriate stamp duty need to be paid either prior to, or at the time of electronic execution

of the commercial contract in order for it to be capable for enforcement by a court in India, without having to pay penalty.

As of date, the applicable Indian laws on stamping only enables procurement of electronically stamped certificate, in addition to payment of stamp duty through conventional method such as procuring non judicial stamp paper. Therefore electronic commercial contracts can't be stamped electronically

5.Various kinds of Security Threats:

Security threat is often considered as one of the greatest barriers to e-contract.The following are the various kinds of security threats posted by the cyber space:

a) Cyber Attacks:

Attacks can be classified as executable-based or network based. In the case of theformer, the attack happens only when a program is executed on the targeted computersystem through either of the following:

- **Trojan** -computer program that appears to have a useful function, but also has hidden and potentially malicious functions that evade security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program.
- **Virus** - a program fragment that is attached to a legitimate program with the intention of infecting other programs. It is hidden, self replicating computer software usually malicious logic, that propagates by infecting, i.e., inserting acopy of itself into and becoming part of another program.
- **Worm** - a computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.
- **Spam** - is also a major source of cyber attacks. Unsuspecting users become victims as soon as they click on attachments.

b) Hacking:

Externally accessible systems are targets of hacking. Hackers can deface websites and steal valuable data from systems resulting in a significant loss of revenue if it is a financial institution or an e-commerce site.

c) Weak Authentication:

Security handling teams estimate that many incidents stem from the use of weak, static passwords. Passwords on the internet can be cracked in a number of different ways.

d)Phishing:

It is the creation of e-mail messages referencing web pages that are replicas of existing sites to make users believe that these are replicas of existing sites to make users believe that these are authentic sites. Unsuspecting users are made to submit personal, financial, or password data to such sites from where the data get directed to fraudsters chosen sites.

e) Spoofing:

The IP address of a host is presumed to be valid and is therefore trusted by TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) services.IP spoofing is used by intruders to gain unauthorised access to computers. Messages are sent to the computer with the sender IP address of a trusted system. Packet headers of the message are modified to make it appear that the message is coming from a trusted system.

f)Credit Card Fraud and Theft of Customer Data:

Almost all B2C purchase transactions involve credit cards. An e-business that accepts credit cards in payment for goods and services, must secure the credit card information in transit to its website, and it must secure stored credit card information.A hacker can break into a database server and steal thousands of credit card numbers and other information in a matter of moments and an e-business might not even recognise that the hacker was there.

g) Data Diddling:

One of the most common forms of computer crime is data diddling – illegal or unauthorised data alteration. These changes can occur before and during data input or before output. Data diddling cases affect banks, payrolls, inventory records, creditrecords, school transcripts and virtually all other forms of data processing known.

h)Web Jacking:

This occurs when someoneforcefully takes control of a website by cracking the password and later changing it. The actual owner of the website does not have control over what appears on the website.

Conclusion:

The IT laws of India have gone a long way since the IT Act was introduced in 2000. However, many aspects of an Online Contract, in particular, the requirements of signature and stamping, remain uncertain and confused. The current trend of demonetizing and digitalization seems a necessity, and we sincerely hope that the government would take appropriate action in that regard, to eradicate all uncertainties in relation to the validity of e-contracts.