

The problems associated with e- contracts essay sample



**ASSIGN
BUSTER**

E-Contractual agreements a complex issue which is unprecedented in the law. The court itself is in dilemma about the latest developments in the technology in terms of Computer software, hardware or internet transactions. My paper discusses and analyses the pros and cons of an online contract in validating it. It covers issues in e-contract, holding of unconscionable terms like that of ' doctrine of unconscionability. My observation is that the development of cyberspace has revolutionized the new legal theories and hence new laws are needed to govern e-contracts. This paper also gives the comparisons and the pros of cons of the existing laws and some proposed laws. The final message says that though there are some differences between E-commerce contract law and contract law in the present nuclear world, but all these differences can be minimized once all the players of the game will be ready to play with the new rules pertinent to an electronic environment also the law will enforce electronic agreements as long as they do not suspect that one party is using the electronic environment to engage in subterfuges.

Introduction: Contracts has become an argumentative issue mostly when it talks about online transaction. Contract is a legal agreement involving parties, activities, clauses and payments. Signed between two or more parties to create business relations or legal obligations between them, a set of activities to be performed by parties satisfying a set of terms and conditions (clauses), whereas an E-Contracts is a contract modeled, specified executed, controlled and monitored by a software system. A number of business partners are involved in E-service environment, workflow, hence inter-operability in such an environment is an important issue Always the

goals of e-contract remains to have precise specification of the activities of the contract, so as to map them into deployable workflows, and to provide transactional support in their execution.

All the activities in a contract are complex and interdependent and are to be executed by different parties autonomously and in a loosely coupled fashion. They may be compensated and/or re-executed at different times relative to the execution of other activities. Both the initial specification of the activities and the later verification of their executions with respect to compliance to the clauses are tedious and complicated. During my research work on this topic I came to the conclusion that an e-contract should reflect both the specification and the execution aspects of the activities at the same time, where the former is about the composition logic and the latter about the transactional properties. Hence to substantiate my statement, I propose a multi-level composition model for smooth running activities in daily e-contracts.

Comparisons

- Shrink-Wrap Agreements vs. Click-wraps and Boxtops

In Shrink-Wrap Agreements Terms are expressed inside a box in which goods are packaged and the party who opens the box is supposed to agree to the terms by keeping whatever is in the box. whereas Click-wraps take place when software is downloaded from a web site. In Box-tops are terms of the contract found in the bottom of a box that contains the product Most X-wraps are made by manufacturers and are applicable to end-users. In many case in Shrink-Wrap Agreements the court has enforced the terms of shrink-wrap

<https://assignbuster.com/the-problems-associated-with-e-contracts-essay-sample/>

agreements just the same as the terms of other contracts. shrink-wrap agreements are agreements that accompany over the counter software “ sales” , which are really licenses to use the software with substantial restrictions on use such as : Copying, decompiling, altering and distributing. It also includes terms like arbitration clauses and forum clauses which preclude going to court if the product does not perform as expected the agreement. Warranty disclaimers are prominent features under Common Law of Contracts. A contract is formed when an offer is made by an offeror or who intends to make an offer and The terms of the contract are definite also The offer is communicated to the offeree and the acceptance of the offeree must be complete and unqualified. It Cannot include additional terms under Uniform Commercial Code: 2-207it

It allows commercial practice to dictate major changes to basic contract law under the current UCC, which governs the sale of goods. An acceptance could have additional terms as long as these terms did not materially alter the contract and the offeror could object There are some other qualifiers regarding the form of the offer and acceptance under Revised Article 2 of the UCC : Section 2-207 says that Under the proposed revisions, an acceptance could have additional or different terms and still form a contract. The terms in the contract are composed of the terms the parties agree upon and Additional terms become part of the contract to the extent that they agree with the contract. If the additional terms are expressly agreed to terms not in the agreement are to be supplied by the UCC gap fillers. Also further, under the proposed revisions, additional terms could be included even though the terms are material in Shrink-wrap, click-wrap, and

box-wrap agreements. Here a customer pays money and receives the product before (s)he becomes aware of all the terms in the contract and Customer is bound by these additional terms in the contract :

Formation of contracts in cyber space in this contract a customer must be given notice of the additional terms also. The contract must be written in understandable terms and the customer must have an opportunity to inspect the terms in the wrap agreement There must be an unambiguous and no burdensome way of returning the item if the customer does not agree to the X-wrap terms. Moreover all money received from the customer must be refunded, unusual terms should be highlighted and not buried in fine print. Lycos is best example to under click-wrap agreement.

Online Contracts: Four levels of security:

While entering into an online contract, following degrees of security is to be seen : The first level would exist if a party accepts an offer by merely clicking on ' I agree' button on the computer screen. The second level would be if secrets were shared between two contracting parties e. g. by the use of password or credit card number to verify a customer's intention that goods or services are to be purchased. The third level is achieved through biometrics, which involves a unique physical attribute of the contracting party, and is extremely difficult to replicate by a would be cyber-thief. for example voice pattern, face recognition, scan of retina or the iris within one's eye ball. In all these cases a sample would be taken from a person in advance and used for later comparison with a person purporting to have same identityforexample if a persons handwriting was used as the biometric

identifier, the ' shape, speed, stroke order, pen pressure and timing information during signing will be recorded and this information is impossible for an imposter to duplicate. on the other hand biometrics has some weaknesses too like in comparison with digital signatures a).

The attachment of the person's biological traits to a document does not ensure that encrypting the resulting message through the hash function at the document has not been altered². b), the recipient of the document must have these two weaknesses and most seem to view the digital signature as preferable to biometric identifiers, the Fourth level is the digital signature as it being more complex than the earlier ones discussed here , in this method entire document which is the sequence of bits and is created by running an electronic message through a one-way hash function then encrypting the resulting message digest with sender's private key. It has advantages over the other forms of digital signature like it verifies authenticity that the communication came from the designated sender, it verifies the integrity of the content of the message by giving the recipient assurance that the message was not altered.

UETA allows the following as electronic signatures: Encrypted digital signatures, names at the end of emails, a click on a web page, if the click includes identification of the person also identification is accomplished through passwords the ways by which digital signatures is considered as legal are : Passwords, hardware that verifies identity-retinal scanners and other such devices also the third party services such as Certification

Authorities as per Article 2 of the UCC which deals with the sale of goods is being revised to accommodate sales of goods A new Subpart B has been <https://assignbuster.com/the-problems-associated-with-e-contracts-essay-sample/>

added to deal specifically with Electronic Contracting which is Uniform Computer Information Transactions Act (UCITA) it allows a mass market licenses-sales to consumers or at the retail level broadly these are X-wrap agreements which says that 1. if the end user does not agree to these terms, the end user has the right to return the product and recover expenses related to de-installation 2. User must have the right to view these terms and the rights to return without charge cannot be waived by the parties .

Rules for electronic contracts:

Attribution to sender: It may be assumed that an e-message was sent by the sender if a). the sender sent it. b). the sender's agent sent it. c). the automatic generation program of sender's information system which sender or his agent programmed sent it or the receiver is able to determine that the transmitter was the sender through use of a procedure or technology which was agreed previously by the receiver and the sender.

Duplicate e-messages: Here it is an assumption that each e-message is separate and independent from others and receiver is entitled to act accordingly.

Acknowledgement of receipt: If the sender, who has requested acknowledgement of receipt , does not specify the form or method of acknowledgement to be used by receiver, then the receiver may employ 1). Any type of commission , manual or automated; or (2) conduct sufficient evidence to show the sender that the reception has occurred.

Conditional upon receipt of acknowledgement: In this case if the sender has instructed the receiver that an e-message will have no legal impact until the sender is in receipt of the acknowledgement, then the e-message is assumed not to have sent until the sender is in receipt of the acknowledgement from the receiver.

Acknowledgement doesn't imply accuracy: The receipt of acknowledgement by the sender justifies his assumption that his e-message has been received by the receiver. However the receipt the acknowledgement doesn't justify the sender to assume that his e-message was accurately received.

Time and place of transmission and reception. An e-message will be assumed to have been sent when it enters a computer information system outside the control of the sender or his agent. Here The Time of Dispatch, the Time of Reception and the Place of Transmission and Reception plays an important role. An e-message is assumed to have been sent from sender's place of business or his permanent residence that he had at the time of transmission. At the same time e-message is assumed to have been received at the receiver's place of business or his permanent residence that he had at the time of the receipt. If either the sender or the receiver does not have to place of business or permanent residence, then the applicable place of transmission or reception will be the party's 'habitual residence' at the time of the transmission or reception.

Gaps found:

My survey to various clients proposed that suppose there is an attribution procedure and the consumer makes a mistake by clicking the wrong dot,
<https://assignbuster.com/the-problems-associated-with-e-contracts-essay-sample/>

then under UCITA the consumer is not liable if he or she notifies the other party of the error, causes or returns the computer information and has not used or benefited from the products. Clients say that Click-wraps hinder automated transactions . whereas nowadays many B2B exchanges use offline agreements which raise Conflicts between off line documents and web site agreement (e. g., different warranties), also Conflicts between web site agreement and terms submitted by site users (e. g., term flexibility) is another matter of concern so Enforcement requires evidence of user “ click” or that user must have clicked to complete transaction whereas Click-wraps don’t solve the attribution and integrity issues associated with e-commerce

Observation Through my online survey I found that Click-wraps are more enforceable than browse-wraps as the attracting features of click-wrap include: explicit E-Sign consent to electronic transaction (if applicable)as before transaction which increases security of contract, it also focuses on viewing the agreement before acceptance that is “ I accept” and “ I do not accept” buttons it also includes“ print” button with the agreement terms which has got provisions of rejecting inconsistent or any /additional terms given.

Suggestions: Before entering into any e-contract both the parties should be clear right from onset agreements to given so that forecasting will be done if some glitches in the software are found in future. Also all communications send to a trading partner should be reproducible i. e. Arbitration rather than litigation the terms signed should be agreed by both the parties involved. All electronic data should be reproducible, when necessary paper copies to be made to avoid any ambiguity.

<https://assignbuster.com/the-problems-associated-with-e-contracts-essay-sample/>

Conclusion: My paper gave clear evidence that a person approved a particular electronic document might be gathered in different ways like discussed above in the paper , so signing the document is a social event and not a scientific one. it involves an individual evidence of approval of the document so that someone else can perceive that approval also understand it, and later be able to prove it to the other people if required . But the bonding of a person to the document is never a perfectly reliable process, whatever evidences exists to support the bond is subject to challenge. In other words I have to say that signing documents online involves risk.

Bibliography

1. Note: 17 supra pp. 395-96; and ' The legality of electronic signatures using cyber-sign is well Established', Cyber-Sign, at <http://www.cybersign.com/news news. htm>
2. 2. Pun K. H suprappp. 395-96; and'the legality of electronic signatures using cyber-sign is well established', cyber-sign, at <http://www.cybersign.com/news news. htm>
3. 3. Stephen Blythe E (2006)," Computer law of Tunisia: promoting secure e-commerce transactions with electronic signatures E (2007), Arab law quarterly, vol. 20, 317-344.
4. Stephen Blythe E (2007), " The Barbados electronic transactions Act: A comparison with the US Model statue", Caribbean law Review, Vol. 16
5. 5. United Nations commission on international trade law(" UNCITRAL") , Model law on electronic commerce with guide to Enactment

(hereinafter " MLEC"), G A Res 51/162, UN GAOR, 51 , Supp. no 49at
336 , UN Doc. A/51/49(1996): [http://www.uncitral.](http://www.uncitral.org/English/texts/electcom/ml-ecomm.htm)

[org/English/texts/electcom/ml-ecomm. htm](http://www.uncitral.org/English/texts/electcom/ml-ecomm.htm)(Accessed 25 Oct 2005).

see Stephen E Blythe , Note: 57 supra.

6. Kingdom of Bahrain, legislative DECREE NO. 28 with respect to
electronic transactions , 2002. Art. 5(4); [http://www. gov.](http://www.gov.bh/content/English/HTML/Electronic%20Transactions%20Law%20English.doc)

[bh/content/English/HTML/Electronic Transactions Law English.](http://www.gov.bh/content/English/HTML/Electronic%20Transactions%20Law%20English.doc)

[doc](http://www.gov.bh/content/English/HTML/Electronic%20Transactions%20Law%20English.doc)(accessed 30 July 2006).

7. 7. Simitis S (1999)," Revisiting Sensitive Data", retrieved February
2006 ([http://www. coe. int/T/E/Legal%5Affairs/Legal%5Fco](http://www.coe.int/T/E/Legal%5Affairs/Legal%5Fco%2Doperation/Data%5Protection/Documents/Reports/W-Report%20Simitis.asp#Topofpage)
[%2Doperation/Data%5Protection/Documents/Reports/W-Report](http://www.coe.int/T/E/Legal%5Affairs/Legal%5Fco%2Doperation/Data%5Protection/Documents/Reports/W-Report%20Simitis.asp#Topofpage)
[%20Simitis. asp#Topofpage](http://www.coe.int/T/E/Legal%5Affairs/Legal%5Fco%2Doperation/Data%5Protection/Documents/Reports/W-Report%20Simitis.asp#Topofpage)).

8. Privacy Exchange," Japan Privacy Resource", Retrieved February
2006([http://www. privacyexchange. org/japan/japanindex. html](http://www.privacyexchange.org/japan/japanindex.html)).

9. 9. European Commission," Commission Decisions on Adequacy of
Protection of Personal Data in Third Countries", Retrieved February
2006([http://europa. eu.](http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm)

[int/comm/justice_home/fsj/privacy/thirdcountries/index_en. htm](http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm)).

10. 10. Bygrave L A (2003), Data Protection Law: Approaching Its
Rationale, Logic and limits, The Hague: Kluwer Law International.