

Challenges of Security in the Law of E-Commerce

Mohammad mohammadi

Kar Higher Education Institute, Tehran, Iran
mohammadi.juristic@gmail.com

Abstract: As we know security is an important item in electronic commerce, which is a new commerce. Electronic commerce has a rapid growth in both domestic and international levels. In electronic commerce transaction of electronic documents is occurred. Documents may be important and secret legal contracts, financial transaction, or secret technologies and security has an essential part of such transaction and electronic commerce. This article will challenge the security in electronic commerce.

[Mohammad mohammadi. **Challenges of Security in the Law of E-Commerce**. *Life Sci J* 2012;9(4):193-196] (ISSN:1097-8135). <http://www.lifesciencesite.com>. 27

Key words: Electronic Commerce, Security, Transaction, Law of E – Commerce

1-Introduction

Electronic commerce is a new commerce, and as it grew, the all legal aspects of this new commerce must also be mentioned.

Nowadays most of countries enjoy internet and many people use internet for their business.

Advances in technology and implementation of electronic modes of communication in businesses and market places in general are very popular now. In comparison with paper – based and or telephonic commerce, in electronic commerce no tangible piece of paper is used, so reliance must be placed upon electronic messages, which may be available in an electronic medium or may be printed out. Some legal structures such as writing a signature or parties' internet are considered differently in traditional commerce and needs for some new rules in electronic commerce in obvious.

One item that needs special rules in electronic commerce is security, which we will discuss it in this article.

2- Electronic Commerce

Electronic commerce can be every commercial issue which is done by internet. In electronic commerce, sale or purchases of goods or services are done by internet. Many contracts dealing with export or import of goods are done by internet now. But as we know electronic commerce has a wider aspect that we mentioned. For example produce management, transaction of goods and also services after sale are different aspects of e – commerce. Since servers of internet and data lines make up the internet, in a backbone of the internet, in a broad sense, electronic commerce means doing business over inter connected networks. [1]

Here are a few examples of electronic commerce:

- Accepting credit cards for commercial online sales

- Generating online advertising revenue
- Trading stock in an online brokerage account
- Driving information through a company via its intranet
- Driving manufacturing and distribution through a value chain with partners on extranet
- Selling to consumers on a pay-per-download basis , through a web site

As a whole electronic commerce is a type of business model, or segment of a larger business model, that enables a firm or individual to conduct business over an electronic network, typically the internet. [2]

3- The Need for Security

Concerning about security should be considered as an essential need.

Security cannot be legislated. [3] It is a combination of factors:

- The technology utilized
- Its business implementation
- State of development
- Legal structure

Security and protecting information against theft or alteration is not a simple work.

Secure electronic commerce cannot be achieved merely by legislating those circumstances when requisite “security “ is present and it requires the creation of an entire infrastructure – legal , social, economic , and political – one that is based on practice which recognizes , validates and supports electronic commerce. [5]

As we need a structure to make our business office secure, and that structures are economic, social, political and legal structure, that send polices as needed, arrests trespassers or thieves and bring them to justice through the court system, and

provides us with the services needed to use and enjoy our property, we need a security system that make our electronic commerce secure and safe. I mean in that system we can arrest trespassers or thieves and brings them to justice.

4- Security in Electronic Commerce

By the topics that we mentioned and traditional thought, the desire for security has showed itself in electronic commerce in somewhat traditional ways.

Early on, in the absence of legislative and judicial recognition and validation of electronic commerce and the corresponding lack of industry – wide standards, customs or standards to guide conduct, attempts were made to set the rules for electronic commerce though trading partner agreements between the parties doing business electronically.

Some regional, national or even international models try to make some rules to make electronic commerce secure. I mean in that models and rules uses some technological barrier to make electronic commerce safe and make entrance to electronic documents such as mail boxes hard for trespassers or thieves. Also in those rules crimes related to electronic commerce are described.

The punishments of those crimes are also added.

In the traditional commerce the owner has the right to use and control property and the ability to acquire and hold that property. Ownership of the property is free and clear of the claims of others. Owners can move or transmit their properties. Also they can sale or transfer their property.

In electronic commerce we should make such structures which we have mentioned above. So in electronic commerce secure business means secure ownership, and secure commercial transaction and doing all business matters securely. I want to say that security in electronic commerce means ability to enter into a commercial transaction that proposes an exchange on terms beneficial to each party, whether sales, services, or commodities agreement, with the reasonable. Expectation that it will be performed. Contracts are performed because our economic, social, and legal structures support those types of transactions and provide incentives for performance as well as disincentives for breach. So security in transaction means that transactions will be performed as expected and the stability and certainty that come with this situations.

By recent progress of electronic commerce and international standards for commercial messages, all countries including undeveloped countries should apply these mentioned standards for international transactions. United nations international commerce

commission (UNCITRA) and international chamber of commerce (ICC) have made some rules for electronic commerce.

In the future lawyers should know electronic commerce, and its rules and structure to act as a good consultant in electronic commerce which deals with commercial contracts, selling goods or services and any other commercial matter.

In the electronic environment, what is arguably lacking at the moment is a discernable legal and social structure that allows the parties to adequately access the risk of electronic commerce and to respond by making intelligent choices concerning their own rights and liabilities, including allocation of risk in transaction with others. [7]

Electronic commerce need a complex security, I mean in order to have an secure electronic commerce should for example have some electronic security which fights against electronic viruses or other similar things and by making firewall fights against trespassers and thieves.

Another security that electronic commerce need is legal security. Legal security flows from a legal framework, on that ma, to a large extent, already exist, but to the extent the application of that framework in the online environment is less than clear, the resulting sense of security may be impaired. [8] it must be recognized, however, that legal security is only a part of the overall security picture.

But unfortunately lack of industry – wide standards, or standard to guide conduct, lack of norms and customs (because electronic commerce is a new commerce and customs are not performed) and new rules which still needs completion cannot give us a high level of security in electronic commerce. However some attempts have made recently. For example some regional and national models trading partner arguments , or interchange agreements, were developed to provide commerce with a contractual frame work for facilitating the adoption and use of electronic commercial practice, thereby providing the parties with some degree of certainty as to the term applicable to their transactions.[9]

Although there are differences between various proposed interchange agreements, a key ingredient of virtually all of them was parties' articulation of the technological business electronically. [10]

But now we need to describe some parts of electronic commerce in order to make readers more familiar with electronic commerce, then we will talk about security electronic commerce.

5-Online Contracts

Because internet is only a communicative device, in first look someone may think that there is no differences between contracts which are made in

internet and electronic commerce with contracts which are made otherwise, and in traditional matters. It is correct that contracts which are made in internet are contracts anyway and the rules of the law of contracts are applying in them but there are some differences and some points which should be mentioned in order to find electronic commerce contracts out well which are listed as bellow:

- In the making electronic contract process some mediums such as ISPs, portals of parties or third parties etc, are applied. Communications in internet are not exactly compatible with the rules which are applying in electronic documents in real and traditional commerce.
- There are some rules which should be obeyed in traditional and real commerce, for example, some contracts are legally binding only if they are performed written and then are signed by the parties – only in these mentioned manner those contracts are formal, but what about electronic commerce and contracts which are made in internet? Written from a signing such contract are an issue which should be discussed. I mean how they can be in written formed and be signed?
- Online selling has its especial rules which differ from traditional commerce.
- When a contract has a foreign element finding the applicable law and the court or courts which has or have competence are important matters.
- We know that there are some rules to find the mentioned issues out in traditional and real commerce, but in contracts which are made in internet answering to those questions are different and rather difficult.

6-1- Contract Making

Some essential rules and topics related to real or traditional and electronic contracts are the same-every contract needs offer, acceptance and intend.

But although electronic contract needs mentioned items, we cannot solve the problems which occurred in these contracts by the rules which are applying in the real contracts.

6-2- Offer and Acceptance

As we know making a contract has two stages:

Offer that in this stage on party of the contract offer a contract to another party. Offer can be in written or orally, besides it can be implied or express.

Acceptance which in this stage the party that receives the offer accept the offer and its conditions if it has any condition. It is mentioned that acceptance should be unconditionally, and conditional acceptance is itself an offer.

For example in the law of England offer is open unit it is accepted or refused, unless conditions or document proves otherwise. And another party can accept the offer any time. Unless this time has some conditions. Also laps of an offer are valid if the party receives the note related to laps of offer. [11]

Every country has some rules related to these issues, but such rules can be applied in contracts which have been made in electronic commerce when we understood the messages of offer and acceptance in which period of time have legal effect. Even the rules of offer and acceptance may be different. In the law of England there is a doctrine which describe that written contract acceptance occurred when it is send even if has not been received yet. [12] if we accept this thesis in electronic commerce, when the message receptacle acceptance is send, acceptance is occurred.

6-3- Electronic Signing

As a rule sign of a contract is valid when:

- Identifications of signer are clear.
- The signer has intended to sign.
- The signer intended to accept the conditions of the document which is signed.

Signers are made by hand can be recognized, but electronic signers cannot shows the identification of the signer by itself. Even by using codes, we can find out that the person who knows the code has sent the messages, and it does not shows the identifications of the sender.

Nowadays there are some organizations and institutes which survey the validity of the electronic signs. When these institutes accepts the validity of the signs provide a certification of the sign which proves the identification of the signer. [13]

7- Vulnerabilities Related to Security

Although legislation try to provide some rules. Which should be obeyed by the parties and these rules make electronic commerce safer, there are some inevitable failures. For instance a user should use a website and at some point identify himself to the site. Typically, authentication begins on user's home computer and its browser. Unfortunately security problems in home computers offer hackers other ways to steal e-commerce data and identification data from user. Some current examples include a popular home – banking system that stores a user's account number in a web "cookie" which hostile web –sites can crack. [14]

Ineffective encryption or lack of encryption for home wireless networks [15] and mail – borne viruses that can steal the user's financial data from the local disk. [16]

Accordingly, an electronic commerce merchant's first security priority should be to keep

the web servers archives of recent orders behind the fire wall.

8- Legislating for Security

When the UETA drafting committee was first established, the assumption given to committee was to avoid inconsistency with the revisions being proposed to the uniform commercial code and in particular article 2B which add some security procedure ore as it calls security attribution to UETA rules . [17]. Theory has diverged from practice, as illustrated by article 2Bs adoption of a presumption approach. [18]

But the question if certainty under Article 2B gives the user any greater assurances that what is mentioned under UETA still remains.

Proponent would still have to prove that there was a method adopted by the parties to authenticate the message as that of the sender, which the method adopted as an authentication device, and that under the circumstances of the transaction in fact operated reasonably as an authentication device. [19]

So can the commercially reasonable security procedure rules help the litigant with the issue of burden of proof.

As was observed in the context of the UETA, a rule placing the risk of loss on the person requiring use of a specified security procedure might indeed discourage people from designating certain procedures, a variation of this provisions in Article 2B was deleted at the drafting committee s last meeting for this reason. [20] But still Article 2B may not encourage the use of mentioned procedures in some aspects.

9- Conclusion

Security in electronic commerce is a multi issue matter, and cannot be solved only by legislation. Some technological issues should be considered.

The relationship between law and these other issues such as security should also be considered. I mean there should be communications between law officials and technology experts in order to provide useful codes.

Besides some attempts should be done in technology in order to make e – commerce safer and

legislative organs use expert lawyer in this topic to provide rules and codes which encourage people to use them.

References:

- [1] – Define E– Commerce in www.umsl.edu/~siegelj/course5890/definitions.html
- [2] – Electronic Commerce – E Commerce in www.investopedia.com/terms/e/ecommerce.asp#a*zz1zpuptkjt
- [3] – Boss , Amelia H. , Searching for Security in the Law of Electronic Commerce , Earle Mack School of Law at Drexel University , from the Selected Work of Amelia Boss , January , 1999,p.590.available at : http://works.bepress.com/amelia – boss/4
- [4] –Ibid
- [5] – Ibid, p.591
- [6] – Ibid, p.593
- [7] – Ibid, p.592.
- [8] – Ibid.
- [9] – Ibid, 593.
- [10] – Ibid, 594.
- [11] – Byrne v. van Tienhove,1880.
- [12] – Household File Insurance V. Grant, 1879.
- [13] – Lazarus Estates Ltd V. Beasley (956).
- [14] – Graves , P., and Curtin, M, Bank One in Line Puts Customer Account Information as Risk, 2000. Available in www.interhack.net/pubs/bankone.online.
- [15] – Borisov, n., Goldberg., and Wagner, d., Intercepting Mobile Communications : in Insecurity of 802.1 Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking 2001, P.180- 189.
- [16] – Robert, P., Bugbear Virus Spreading Rapidly, PC World Online, October 2, 2002, in rsasecurity.com/rsalabs/faq/5-3-1.html.
- [17] – Boss, Ibid, p.615
- [18] – Ibid.
- [19] – Ibid, 619.
- [20] – Ibid, 620.

2/20/2013