Journal of Politics and Law; Vol. 9, No. 7; 2016
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Data Privacy in Electronic Commerce: Analysing Legal Provisions in Iran

Parviz Bagheri[1] & Kamal Halili Hassan[2]

[1] Ilam University, Iran

[2] Kamal Halili Hassan, Faculty of Law, Universiti Kebangsaan Malaysia, Malaysia

Correspondence: Parviz Bagheri, Ilam University, Iran. E-mail: p.bagheri@ilam.ac.ir

Received: February 15, 2016 Accepted: August 21, 2016 Online Published: August 30, 2016

doi:10.5539/jpl.v9n7p133 URL: http://dx.doi.org/10.5539/jpl.v9n7p133

Abstract

This article discusses the legal protection of data privacy in electronic commerce in Iran. Currently, there is a gap in respect of data privacy protection in Iran as there is no specific privacy legislation in force. Consequently, e-consumers dealing in internet commerce are less protected. However there are rules and regulations in the laws in Iran such as the Islamic Republic (IR) of Iran Constitution, Computer Crimes Act, Penal Code, and Civil Liability Act which relate to privacy in general, although not directly related to data privacy in e-commerce. The Electronic Commerce Law (ECL) is the main legislation in Iran which contains some provisions on personal data privacy. This article discusses the relevant provisions in the ECL pertaining to data messages and privacy and interprets its various meanings to determine whether they are in line with well established principles found in good data privacy protection measures.

Keywords: data protection, internet commerce, Iran, privacy, Electronic Commerce Law

1. Introduction

Privacy is a person's state of having their own personal space or data which they do not want to share with others (Xue, 2010). It is an already well established domain recognized by various laws, cultures, and religions, and is relevant to every human activity. In the context of internet transactions, it is critical that data privacy especially that of the purchaser is properly guarded by the website owner. Data protection is not only about keeping personal information confidential but also about creating a trusted framework for the collection, exchange, and use of personal data in online transactions (Munir & Yasin, 2010a). Data protection laws must strengthen consumer confidence in e-commerce and online transactions as a prerequisite for sustainable growth in electronic commerce. Without such protection, consumers will not visit or shop at a website, nor can websites function effectively. The technology too is a significant enabler, and the pace of change in the virtual world is staggering (Litan, 2001). With the development of the World Wide Web (3W), audiences are becoming networks of communities and people are able to access goods and services in wider and bigger contexts. The success of social networking websites such as *MySpace, Face book*, *Twitter*, *YouTube,* and *Bebo* or even *eBay* and *Amazon.com* depends on users posting a whole range of online information on their personal interests, occupations, and personal status (Sparrow, 2010). Virtual worlds are the next stage of development of social networks, and could become the first point of contact between companies (businesses) and customers. Virtually every e-commerce transaction involves the transfer of personal data and needs regulation by the laws of the state.

Privacy is a fundamental human right as provided in Article 12 of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), UN Convention of Migrant Workers, UN Convention on the Rights of the Child, Article 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, and various other regional and international treaties. As "privacy" and "data privacy" have very broad meanings, we will only focus on informational and general data privacy of consumers in online business transactions. It concerns the rights individuals to have control over their information, and this informational privacy is also known as data protection (Hassan, 2012).

E-commerce in Iran has already experienced a good number of transaction activities although not as prolific as in developed economies. Online transactions in Iran totalled USD100,000 in 2010 . In contrast, in developed countries, 70% of people use online transactions. Research conducted in 2013 shows that 43% of online

activities in Iran relate to online shopping (Bagheri & Hassan, 2015a). The rights of e-consumers in Iran are protected by the Electronic Commerce Law and Consumer Rights Protection Act 2009 which has helped to some extent in addressing legal problems relating to business conduct via the internet (Bagheri & Hassan, 2012b). Esfandiari (2011) however points out that Iran needs to reform the physical structure and nature of its industries and the processes of marketing, insurance, and after-sale support services to further the growth of e-commerce and this include the protection on data privacy. As discussed below, privacy issues, being the main pillar to e-commerce, are not adequately addressed in Iran.

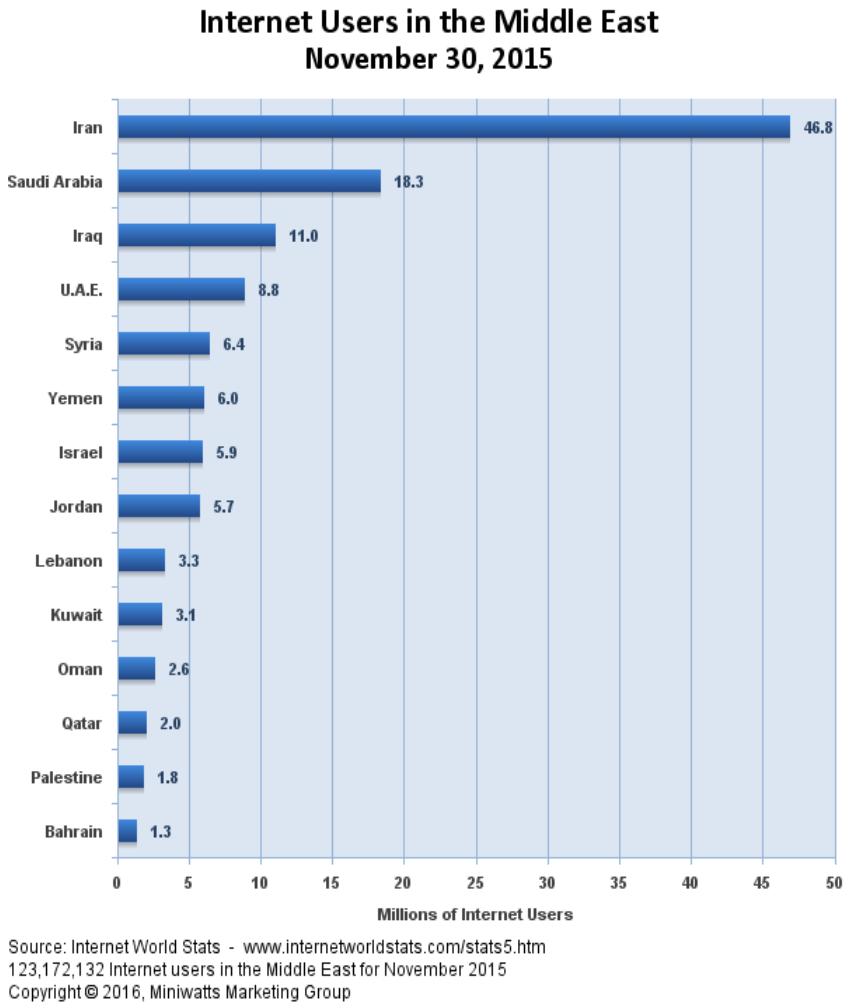

Figure 1. Above shows that among Middle East countries, Iran is the highest users of internet and surely e-commerce also strives in Iran

2. Literature Review

In his article, "Privacy and its protection in Iran, Islamic law and comparative law", Ansari Bagher (2004) examines Iranian information society in a global context. He reviews recent initiatives of the Iranian government aimed at facilitating the development of e-commerce in Iran and examines electronic contracts and the United Nations Convention on the use of electronic communications in international contracts. Although he only provides limited information on the conditions of an electronic contract he points out some key provisions in Islamic law regarding the protection of the data privacy. Through verses of the Holy Quran and Hadith (the teachings and conduct of the Islamic holy prophet) such as "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded" (24:27), he tries to show that Islamic law places special emphasis on respect for privacy. The author also believes that data privacy protection in Islamic law far antecedes other legal systems. However, finding overall legislation in the legal system of the Islamic countries regarding data privacy is challenging.

In his book titled "E-Commerce Crimes: Computer Crimes in Domain of E-Commerce" Javidnia Javad (2009) describes the history of e-commerce and judicial interpretations of the Iranian Penal Code articles with the ECL 2004. Briefly, the author deals with the breach or violation of consumer rights and advertisement rules from a criminal viewpoint. According to the provisions of the code, the investigation and gathering of information, except in public offenses, are prohibited. In circumstances where an offense is of an individual or private nature and has not been committed publicly, its disclosure (with intent to cause the offender penalization) is not only disapproved of, but considered tantamount to the dissemination of vile deeds and therefore a sin. He tries to clarify the criminal guarantees of the Iranian Penal Code on data privacy as stated in the Penal Code Articles 570, 572, 573, 574, 580 and especially 691, 692 and 694.

Aslani Hamidreza (2006) in "Information Technology Law" stresses that Allah has prohibited trespassing against truth and reason, which is closely related to the violation of privacy. He states that each individual has the right to privacy and may not want others to have access to certain information their life. He analyses privacy in the information society and personal data protection especially in the context of the meaning and principles governing data privacy. He then declares that the right to personal privacy including data privacy takes precedence over substantial rights such as land interests. He states that under Islamic principles, the right to privacy is one of the fundamental components addressed in divine authorities to ensure a peaceful and harmonious life for everyone in the society including e-consumers.

Abbasi Alireza (2007) writes about "E-commerce Development in Iran" which traces its development and recognizes Iran's E-Commerce Law as an important piece of legislation on e-business activities. He analyses the provisions of the ECL and considers its enactment as a positive step towards cooperation with other nations through e-commerce transactions. However, the article only states the provisions of the ECL and does not explore the inadequacies of the law especially on privacy.

3. Methodology

Methodology in legal research is different from other social science research. Legal research is primarily premised on the analysis of legislation and case-laws and uses cases and the legislation as the main instruments. Legal research and writing is traditionally anchored on doctrinal research which refers to a new, thorough, systematic, investigative, or theoretical analysis. Its aim is to explore, revise, add value, and improve the concept, theory, principles, and application of law. In other words, legal research usually adopts the methods of theoretical, doctrinal, or legalistic analysis which emphasizes legal problems and issues. Using the content analysis technique, legal research aims to resolve problematic situations and identify elements that constitute such problems and the regulations relating to them. However, modification in legal research method is unavoidable in certain circumstances especially in legal system of developing economies where judicial decisions are minimal or non-existent especially those pertaining to new legislation. In this paper, such limitations exist due to the fact that privacy laws are still in their infancy in Iran. There have been no cases decided by the courts on privacy issues and, as such, no discussions can be conducted. Within this limitation, this article is mainly based on a discussion of the provisions of the relevant legislation. In addition, establishing hyphoteses is uncommon in legal research; instead it is substituted with research questions. Thus the research questions in this articles are: (i) Since Iran has no specific legislation on data privacy, is the ECL, which contains some provisions on data messages, adequate for protecting e-consumers?; (ii) does the provisions in the ECL fulfill salient principles of data privacy usually found in other developed jusrisdictions?

4. Privacy Provisions in the General Laws in Iran

In Iran there is a major gap in respect of data privacy protection as specific legislation on it is nonexistent. However there are rules and regulations pertaining to privacy in general provided in other laws such as the Islamic Republic (IR) of Iran Constitution, Electronic Commerce Law, Computer Crimes Act, Penal Code and Civil Liability Act which have, to a certain extent, a bearing on personal or data privacy. However, the Electronic Commerce Law (ECL 2004) has the most provisions which deal with data privacy in commercial transactions and as such, reference has to be made to the ECL (explained further below).

The IR Iran Constitution refers to privacy in general. It acknowledges the personal dignity of citizens and privacy of communications, but does not specifically address protection of personal information. Article 22 the constitution states that, "The dignity, life, property, rights, residence, and occupation of the individual shall not be violated, except in cases sanctioned by law". The constitution explicitly does not protect privacy although as the supreme law of the land it contains the principles relevant for such a purpose (Ansari, 2004). Like the constitution, the Iranian Criminal Procedure Code 2000 also does not clarify on privacy protection and only refers to some related aspects such as home and communication privacy. Articles 12, 13, 14, and 16 of the

Iranian Computer Crimes Act (CCA) 2009 refers to the rights of individuals including consumers to have privacy, and sets criminal penalties for those who invade individual privacy through the use of electronic systems. Based on those provisions, any breach of privacy is treated as defamation. Cases involving oral or printed disclosure of personal information, fabrication of facts to publicly vilify the dignity of persons, or damage the reputation through insults and defamation, and casting aspersions on individuals are considered a breach of reputational rights (Javad, 2009). Although the CCA 2009 mainly covers criminal acts, persons committing e-commerce offences can also be charged under it.

In the meantime, the general principles of the Iran Civil Code do not include privacy as an independent civil right. Article 1 of the Iranian Civil Liability Code 1960 states that, "Any person who intentionally or due to his negligence, injures the life or health or property or freedom or prestige or commercial fame or any other right established for the individuals by virtue of law, as a result of which another one sustains materially or spiritually losses, shall be liable to compensate the damages arising out of his action." The Iranian Penal Code 1982 defines various offences, penalties, and steps to be taken for ensuring the privacy of the individuals. Article 640 provides criminal punishments for those who invade public ethics and dignity stating that "The following people should be imprisoned from three months to one year and pay a fine of 1,500,000 to 6,000,000 *Rials* and also be flogged up to 74 lashes, or any or both of these punishments

a) Anyone who with the purpose of trading, public showing, or distributing publicizes any picture, text, photo, drawing, article, newsletter, newspaper, movie, or any other thing that violates public morals;

b) Anyone who is included in the circulation of the above items."

Article 641 of the Penal Code refers to the act of a person who through the use of a telephone or other telecommunication systems interferes with or disturbs others, and the offender will be subject to 1 to 6 months imprisonment.

All the above laws only point out some general rules on privacy and respecting the private life of the individuals. Uncertainties remain as to when comprehensive legislation will be enacted in Iran that will provide greater protection for personal information.

5. Questioning Data Privacy in the Iranian Electronic Commerce Law

Three particular laws containing provisions concerning the protection of data in Iran are: the Law on Electronic Commerce (LEC), approved in 2004; the Law on Computer Crimes (LCC), approved in 2009; and the Law on Publicising and Access to Data (LPAD), which entered into force in February 2010. Other laws and regulations also require protection of data within a specific context. Private contracts for non-disclosure of information are generally acknowledged based on the freedom of contract principles recognised under the Iranian Civil Code. According to Article 58 of the LEC, "storing, processing or distributing private data messages which may reveal tribal or ethnic origins, moral and religious beliefs, ethical characteristics and data messages regarding the physical, psychological or sexual condition of people, without their explicit consent is illegal." A "data message" is defined as any representation of facts, information and concepts generated, sent, received, stored or processed by use of electronic, optical or other information technology means. Violation of the above rules is punishable by a prison sentence of one to three years. Article 16 of the LCC provides that anyone who, by use of computer or telecommunication means, publicises or makes accessible the film or picture or sound or personal or family secrets of another person without his or her consent and causing loss or damage to the relevant individual or violating that person's dignity will be sentenced to imprisonment for between 61 days and six months or fined Rls 1,000,000 to 10,000,000. Unauthorised access to and distribution of secret information (i.e. information which, by its disclosure, would harm national security or the public interest) is also an offence under the LCC. Under the LPAD, data is defined as "any data incorporated in a document, or saved in the form of a software or recorded through any other medium". LPAD categorises the data into "private information" (including personal information such as first name and surname, home and work addresses, individual habits, bank accounts etc.) and "public information" (such as 144 Norton Rose Fulbright – July 2014 Global data privacy directory rules and regulations, national and official statistics and figures etc.). According to LPAD, while private information can only be accessed by the person to whom the data belongs or from the authorised proxy, public information can be accessed freely (except in cases prohibited by relevant laws). LPAD recognises the right of persons to claim damages (based on the Law on Civil Liability) in case any loss or damage is suffered as a result of the publication of untrue data or true data in breach of the provisions of the law. A breach of LPAD is regarded as a crime resulting in a financial penalty of a sum between Rls 300,000 and Rls 100,000,000. Where other laws impose higher penalties for the same offences, the higher penalty will apply. In addition, the Islamic Punishment Act penalties the disclosure of information obtained by doctors, pharmacists, surgeons and other trusted people

in the course of carrying out their work. The collection of classified information to distribute is also an offence in certain circumstances. However, hacking and infringement of the data privacy of the internet and social users in Iran is a serious threat for the cyber actors. The ease with which data can be acquired and disseminated across the Web, and the peculiarities of the electronic environment have led to growing concerns from many potential customers over disclosing personal information to e-goods/services providers in Iran.[1]

http://www.nasimezanjan.ir/

The above diagram shows the rank of Iran among the countries of the world in terms of social network (telegram) trafficking. At the mean time recently the private and family pictures of a football player have hacked and disclosed illegally through the use of telegram social network. [2] Another example happened when one of the employees of a private company which conducts as a Payment Service Provider (ISP) has disclosed the information of more than 3 million customers of about 20 banks in Iran.[3] This information includes the number and Pin Code – a secure code consists of four digits- of the customers. This disclosure of the information may not be considered as the breach of data privacy of the customers but it shows that the banking system shall apply a more secured policy in order to protect the data of the customers.[4]

The research questions to determine whether the ECL fulfills the common principles of providing good legal provisions on data privacy are as follows:

(i) To qualify as "personal data," the data must relate, either directly or indirectly, to a data subject who can be identified from the data. It must also be capable of being recorded and be subject to automatic or manual processing. The ECL as a specific law is the only legislation that addresses privacy issue and the protection of the private data messages. Article 2(a) of the ECL defines "data message" as: "any representation of facts, information, and concepts generated, sent, received, stored, or processed by use of electronic, optical or other information technology means". This definition is broad enough to cover data message in electronic transactions. Iran has provided legal provisions on collecting, processing, and storage of information by the providers of goods and services, and established penalties for the breach of these rights. The ECL provides e-consumers room to demand respect of their personal dignity in purchasing and using commodities and receiving services. Article 58 of this law states, "Storing, processing or distributing private 'data messages' which may reveal tribal or ethnic origins, moral and religious beliefs, ethical characteristics, and 'data messages' regarding the physical, psychological, or sexual condition of people, without their explicit consent is illegal". Article 60 refers to medical or health records and states that, "Storing, processing, or distributing 'data messages' of medical or health records

[1] For example, many network advertisers and sellers collect anonymous information by using 'cookies' to track the consumer's movements on the seller's site. A cookie is a file on the user's computer or a computer data storage program that can be and is accessed by websites that a user visits and enables the website to record, using information on a visitor's hard drive his /her online activities. A cookie does not contain information about the consumer.

[2] http://www.nasimezanjan.ir/

[3] Asre Iran Electronic Newspaper, Available at: http://www.asriran.com, (15/04/2012)

[4] Asre Iran Electronic Newspaper, Available at: http://www.asriran.com, (15/04/2015)

are subject to the regulations in accordance with Article 79 of this Law." Article 79 provides criminal sanctions to those violating the above such as imprisonment of one to three years. It is argued that the ECL does not merely protect personal data of the individuals including consumers, and that only sensitive personal data such as medical and health data are covered. It should be noted that the success of any legislation will be measured by its implementation and compliance, and in this context the ECL suffers from the lack of enforcement.

"Sensitive personal data", which require explicit data subject consent, include medical history, religious beliefs, political opinions and the commission or alleged commission of any offence. The ECL does not protect mere personal data of the individuals including consumers but does allow for sensitive personal data such as medical and health data to be protected. It does not differentiate between sensitive and normal data of the data subject nor does it clarify on what constitute exceptional circumstances such as public interest under which the data may be obtained without the consent of the data subject. Moreover, the ECL is silent regarding personal data relating to the criminal defamation of individuals. Although the ECL provides that before processing information the consent of the data subject shall be obtained, the data subject is allowed to withdraw his consent at any stage of the transaction. Articles 67 and 68 of the ECL refer to electronic fraud and forgery declaring them as criminal acts, but it is better for the law to declare mere unlawful entrance as criminal. In other words it should declare any entry into the electronic systems as an unlawful act

(ii) Personal data must be processed fairly and lawfully and this requirement should be the primary overarching principle of any legislation. Accordingly, if the data controller or service provider fails to apply the privacy practices it promotes, the regulators treat that failure as a deceptive trade practice that misleads and harms consumers. Articles 79 and 61 of the ECL has put the duty of compilation of relevant rules and regulations of the law to the relevant institutions, meaning, some ministries such as Ministry of Industry, Mine and Commerce, the Supreme Council of Information Technology and Council of Ministries. Even 8 years after the enactment of the law and although many e-businesses have established their presence in cyberspace through websites, some of the memorandums have still not been prepared. The businesses collect information online but their websites mostly do not have any policy/privacy statement or at least the policy is not available online. In addition, some privacy/policy statements are unclear or misleading and sometimes do not mean anything. In some cases, the policy statements are brief and incorporated into the provisions of ECL or any other legislation. Some of the banks such as *Meli, Tejarat, Saderat,* and *Melat* have privacy policies which are not secure and do not conform to legal obligations as well as are detrimental to consumer interests. Recently an employees of a private company which acts as a Payment Service Provider disclosed the information of more than 3 million customers of about 20 banks in Iran (Asreiran, 2012).

(iii) The data not only should be obtained lawfully but should be obtained for specific and lawful purposes. Therefore any data held by the controller must be specified in a notice to the data subject. In order that data is obtained legally, financial institutions in Iran require the consumers to use a Pin or tracking number as a secure code. For example, the number and Pin Code as a secure code of a consumer consist of four numerical digits. This disclosure of the information may not be considered as the breach of data privacy of the customers but it shows that the banking system should apply a more secured policy to protect customer data. An important principle of fair and good information practice is that an Internet Service Provider (ISP) or an e-merchant should take security measures to protect consumer information or data from loss, misuse, and alteration. Companies and even banks in Iran are still not adequately secured and equipped with measures to protect consumer rights in terms of data protection in online transactions. Another important issue that threatens consumer privacy in online transactions is unsolicited commercial messages or email (or 'spam' as it is commonly known), typically of a marketing or malicious intent, not requested by the recipient. There are two legal approaches to control unsolicited commercial messages: opt-out and opt-in. The written notice shall be in national and English languages, and individuals should be provided with clear and readily accessible means to exercise their choice in both languages.

(iv) The notice should describe the information that is being collected, identify who will have access to it, and how it will be used. Personal data requests should also be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed. Article 55 of the ECL provides that the suppliers shall provide consumers with the required arrangements to enable them to choose whether to receive the advertisements at their mailing or e-mail address. In this case, the provision does not choose any of the opt-in or opt-out approaches. However, the by using the term "enable them to choose whether to receive" it can be considered that the law tends to apply the opt-out policy which cannot protect consumer rights in terms of data protection in online transactions. Under Article 70, the law provides for a 20 million to 100 million *Rial* penalty for violators and those who breach the provisions of Article 55. Iran does not have any specific data protection legislation. The ECL is silent on such important matters in online transactions. It is argued that the ECL's provisions are not suited to the electronic

environment taking into account consumer rights especially in terms of data protection (Hamidreza, 2006). It not only ignores the law of competition but also the need for commercial data protection. For example the data of a consumer who is going to become a member of a commercial union is not protected by the provisions of this law.

(v) Personal data shall be accurate and, where necessary, kept up to date. A data user is obliged to correct data it holds should the individual to whom the data relates establishes that it is not accurate, complete, or current. Since the data is collected or obtained from the data subject, data users may argue that they did all that they could reasonably have done to ensure the accuracy of the data at the time. The data not only should be obtained lawfully but should be obtained for specific and lawful purposes. Therefore any data held by the controller must be specified in a notice to the data subject. Article 59(a) of the ECL provides that in collecting data message "its goals shall be specified and clearly described". Article 59(b) ascertains that "the data message shall be collected to the required extent and in compliance with the goals described to the person who is the subject of the data message while collecting the information and be applied merely for the goals set out therein." The terms "required extent" and "in compliance with" are subjective terms and need to be interpreted in a practical sense. Further, Article 59(c) states that, "The 'data message' shall be correct and up-to-date". When the data is incomplete or inaccurate, it would have direct or indirect effects on the data subjects (consumers). For example, a customer who has been discharged from being a bankrupt would still face difficulty in obtaining loan facilities from the bank, if the data pertaining to his credit history has not been updated.

(vi) Processed personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained. Once the purpose for which the data collected is achieved, the data controller should carry out periodic data audits to ascertain whether it needs to be retained. The time for erasing the collected data is not mentioned in the ECL but in Article 59 (d & e) it states that, "The person who is the subject of a 'data message' shall have access to those computer files containing his/her personal 'data messages' and be able to remove or amend partial or incorrect ones", and "The person who is the subject of 'data message', while adhering to the regulations, shall be able to request the complete removal of the computer files of his personal 'data messages'". The article also refers to the consent of the data subject and states, "Upon the consent of the person who is the subject of a 'data message', provided that the content of the 'data message' is in accordance with statute laws of the Islamic Consultative Assembly (Parliament), storing, processing, and distributing personal 'data messages' via electronic means shall be subject to the following terms:

> (a) Its goals shall be specified and clearly described;
>
> (b) The "data message" shall be collected to the required extent and in compliance with the goals described to the person who is the subject of the "data message" while collecting the information and be applied merely for the goals set out therein;
>
> (c) The "data message" shall be correct and up-to-date;
>
> (d) The person who is the subject of a "data message" shall have access to those computer files containing his/her personal "data messages" and be able to remove or amend partial or incorrect "data messages"; and
>
> (e) The person who is the subject of "data message", while adhering to the regulations, shall be able to request the complete removal of the computer files of his personal "data messages".

Iranian law neither clarifies the exceptional issues such as public interests or security instances in which the consent of data subjects may not be necessary nor differentiate between sensitive and normal data belonging to them.

(vii) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. According to the latest regulation in Iran, it is provided that the operators must obtain the addressee's consent before sending any advertisement. The mobile of the individuals has been considered as the private zone and sending any unwanted advertisement (spam) is against the law of data privacy. This rule is applicable from 8 February 2012 (Asriran, 2012). The ECL does not refer to efficient technical and organizational measures in online transactions but Article 59 (e) refers to the right of the data subject to completely erase their collected data. This provision at least ensures the e-consumer that his right to erase his data can be enforced. Article 2 (h) provides that all online transactions must be done through a secure information system which is "An information system that: (i) Is reasonably protected against any misuse or penetration; (ii) Possesses a reasonable level of proper accessibility and administration; (iii) Is reasonably designed and organized in accordance with the significance of the task on hand; (iv) Is in compliance with secure methods". Part (i) of the same Article describes secure method and says it is "A method to authenticate the correctness, the origin and the destination of a "data message", along

with its date and to detect any error or modification, in communication, content, or storage of a "data message" from a certain point. A secure message is generated using algorithms or codes, identification words or numbers, encryption, acknowledgement call-back procedures or similar secure techniques".

The ECL does not point out the non-contractual civil liability for compensating the loss or damage. However, this can be resolved through the general regulations of contractual civil liability such as Article 1 and 2 of the Iranian Civil Liability Code 1960. Article 1 states that, "Anyone who injures intentionally or due to his negligence, the life or health or property or freedom or prestige or commercial fame or any other right established for the individuals by virtue of law, as a result of which another one sustains materially or spiritually losses, shall be liable to compensate the damages arising out of his action". Meanwhile, Article 2 provides that "In the event that the action of the loss inflictor causes material or spiritual damages borne by the loss inflicted person, the court shall condemn him to compensate the said damages after considering the case and establishment thereof. Should the action of the loss inflictor have caused one of the aforesaid damages; the court shall condemn him to compensate the same sort of damages inflicted". However the above uncertainties in the ECL and other laws regarding data privacy especially in terms of consumer protection in the virtual environment makes it important that they are revised in line with the rapid growth and spread of electronic commerce.

(viii) Personal data shall not be transferred to a country or territory outside unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The electronic onward transfer and trans-border data flow of the consumers' data whether inside or outside of the consumer's territory must be prohibited unless protection is guaranteed (Munir & Yasin, 2010b). The ECL refers to the international characteristic of this law and its interpretation and in Article 3 states, "The international origin, the need to promote uniformity in its application, and the observance of good faith should always be taken into consideration in the interpretations of this Law". As a guarantee of the data privacy in the virtual environment Article 67 states that "Anyone who deceives others or misleads auto- processing systems and the like, during an electronic transaction, by misuse or unlawful use of "data messages", programs, computer systems, and means of distance transaction, and committing such acts as penetration, removal, and termination of a "data message", interfering with the application of a computer system or program, etc. and by means of this method obtains property or financial concessions for himself or others, is deemed an offender and in addition to the return of property to its owner is given a one to three year sentence in prison and pecuniary punishment equal to appropriated property". Although the phrase "deceiving" others or "misleading" auto-processing systems, may implicitly include the transfer of the data subject, the ECL does not have any provision regarding the transition of the e-consumer data. It does not refer to such an important matter in cyber arena and leaves the consumers with no protection in this regard.

6. Conclusion

Although the ECL is the best legislation in providing protection on matters relating to data privacy in Iran it falls short in meeting good principles of data privacy protection. The research questions posed earlier can be answered as follows: (i) the ECL, which contains some provisions on data messages, is inadequate in protecting e-consumers. Iran needs specifc legislation on personal data protection; (ii) the provisions in the ECL does fulfill some salient principles of data privacy usually found in other developed jusrisdictions although few principals are missing. For example, it does not completely protect personal data of individuals and only recognizes sensitive personal data such as medical and health data. Moreover, in regard to information collection, the provisions of the ECL do not provide adequate legal protection to e-consumer rights in online transactions. E-business websites collect information online but most of them do not have any policy/privacy statement or at least the policy is not available online. In addition, some privacy/policy statements are unclear or misleading and sometimes do not mean anything. In some cases, the policy statements are brief and incorporated into the provisions of ECL or any other legislation.

Companies and even the banking system in Iran are still neither secured nor equipped with adequate measures to protect consumer rights in terms of data protection in online transactions. Their privacy policies are unsecured and do not conform to legal obligations as well as are detrimental to consumers. The ECL provisions are not suited to the electronic environment. Besides not referring to the law of competition, it also does not cover commercial data protection. It is silent on data protection of minors and especially children. Moreover, it does not refer to efficient technical and organizational measures in online transactions nor clarify exceptional circumstances such as public interest under which the data may be obtained without the consent of the data subject. Moreover, it is silent on personal data relating to the criminal defamation of individuals. In addition to all the mentioned inadequacies, the ECL only provides for criminal enforcement for fraud and forgery while other criminal acts such as sabotage are excluded. The issue of identity theft in online transactions is not covered and Internet users remain exposed to

abuse.

References

Abbasi, A. (2007). E-commerce development in Iran. *Webology, 4*(4).

Asre. (2012). *Asre Iran Electronic Newspaper.* Retrieved April 15, 2012, from http://www.asriran.com

Asriran News. (2012). Retrieved March 10, 2012, from http://www.asriran.com/fa/news/200481

Bagher, A. (2004). Privacy and its protection in Iran, Islamic law and comparative law. *Journal of Law and Political Science,* (66), 1-54.

Bagheri, P., & Hassan, K. H. (2012a). Electronic commerce and consumer protection development in Iran: Policy and infrastructural influences. *International Business Management, 6*(3), 333-339. http://dx.doi.org/10.3923/ibm.2012.333.339

Bagheri, P., & Hassan, K. H. (2012b). E-commerce and consumer protection in Iran: A legal framework. *International Business Management, 6*(3), 317-324. http://dx.doi.org/10.3923/ibm.2012.317.324

Bagheri, P., & Hassan, K. H. (2015). Access to information and rights of withdrawal in internet contracts in Iran: The legal challenges. *Computer Law & Security Review, 31*, 90-98. http://dx.doi.org/10.1016/j.clsr.2014.11.006

Esfandiari, M. (2011). *Internet marketing, Iranian Labor News Agency (ILNA).* Retrieved March 11, 2011, from http://www.ilna.ir

Hamidreza, A. (2006). *Information Technology Law*. Tehran: Mizan Publication.

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law & Security Review, 28*, 696-703. http://dx.doi.org/10.1016/j.clsr.2012.07.006

Javad, J. (2009). *E-Commerce Crimes; Computer Crimes in Domain of E-Commerce*. Tehran: Khorsandi Publication.

Litan, R. E. (2001). Law and policy in the age of the Internet. *Duke Law Journal, 50*(4), 1045-1075. http://dx.doi.org/10.2307/1373102

Munir, A. B., & Yasin, S. H. M. (2010a). *Information and Communication Technology Law: State, Internet and Information, Legal and Regulatory Challenges*. Kuala Lumpur: Sweet & Maxwell Asia.

Munir, A. B., & Yasin, S. H. M. (2010b). *Personal Data Protection in Malaysia: Law and Practice*. Kuala Lumpur: Sweet & Maxwell Asia.

Sparrow, A. (2010). *The Law of Virtual Worlds and Internet Social Networks*. USA: Gower Publishing Company.

Xue, H. (2010). *Cyber Law in China*. Wolters Kluwer Law and Business, China: Beijing.