IMPORTANCE OF SELF-REGULATION IN ELECTRONIC TRANSACTIONS: SAFEGUARDING CUSTOMER INFORMATION AND PRIVACY

I. Alharbi[1], and B. alyoubi[2]
[1]Department of Management Information Systems, College of Business, University of Jeddah, Jeddah, Saudi Arabia
[2]Department of Management Information Systems, College of Business, University of Jeddah, Jeddah, Saudi Arabia

Abstract - *The emergence of electronic transactions has played an incredible role in increasing convenience and ease, in terms of performing purchasing/selling activities from remote location).The research is aimed at assessing the importance of self-regulation in electronic transaction, particular in terms of securing the information and privacy of the customers. However, electronic transactions have also brought several complexities and threats, in terms of protecting customer's information. In this situation, the integration of self-regulations in electronic transactions can be considered as an effective approach for protecting customer's confidential information from unintended threats and risk. This research paper encapsulates brief yet profound information about the relevance of using self-regulatory regimes in electronic transactions. In addition to this, it also includes the illustration of the fundamental elements that are crucial for the development of meaningful self-regulation for the electronic transactions, so as to ascertain the privacy of the customers. The study found that, businesses have started to put especial emphasis on the establishment of self-regulatory regimes, in order to ascertain the integrity of their client's data. Analysis shows that self-regulation is more effective and flexible, as compared to traditional governmental regulations.*

Keywords: Self-regulation, electronic transactions, privacy, information, regime, e-commerce

1 Introduction

The purpose of this research study is to examine and discuss the importance of self-regulation in electronic transactions. More specifically, the research work is intended to recognize the importance of self-regulations in terms of protecting the privacy and information of the customers in e-commerce environment. It has been established from the analysis of the study that was conducted by [5] that advanced information technologies have enabled the businesses to enable their customers to perform their transactions in a more efficient manner. In accordance of the study of [14], online shopping is one of the most desirable options of the customers, as it allows them to purchase their desired products or services, regardless of their geographical location. It is observed that the ease of selling and purchasing goods over the internet has played an inevitable and indispensable role in the development of the electronic payment and electronic commerce services. [24] has stated that customers find electronic transactions as the most efficient and convenient method, instead of visiting the specific location to perform financial transactions. Despite of extensive benefits of electronic transactions, like ease and convenience, a number of challenges are also associated with this technology. One of the most prominent issues that are related to the electronic transactions includes the security of the information and privacy of customer's information [23]. In this regard self-regulation has found to be one of the greatest approaches that may help the businesses in safeguarding the privacy and confidential information of the customers, while performing electronic transactions. In order to present more cohesive illustration of self-regulation and its importance in electronic transactions, the proceeding paper encapsulates its different beneficial aspects that foster customer privacy.

1.1 Research Aim & Objectives

The aim of this research study is to evaluate the importance of self-regulation in electronic transactions. In this regard, the researcher is intended to accumulate pertinent information about self-regulation, in terms of protecting customer privacy and information. Following mentioned objectives are going to be accomplished in the paper, in order to acquire the research aim.

The research will be covering many aspects of the self-regulation in the electronic transactions. The primary purpose of the research will be to understand the privacy of the customers' information in electronic transaction, examining the approaches and concepts of self-regulations. Moreover, the study will also be analyzing the fundamentals of effective self-regulation to safeguard the information and privacy of the customers. In the end the study will also be evaluating and discussing the significance of self-regulation in electronic transactions to protect customer information and privacy.

2 Methods and Materials

The present study has used secondary qualitative research approach. The researcher has adopted this method of research to accumulate pertinent and relevant information about the topic, in a more efficient, cost effective, and well-timed manner. It is significant to bring into the notice that different authentic databases have been accessed by the researcher to gather credible information. Some of the prominent resources that have been accessed include JSTOR, EBSCOHOST, and sage. These resources have commendably contributed in the successful accomplishment of the research objective.

3 Literature Review

3.1 Privacy of Customer`s Information

Type Technological developments have played an inevitable and indispensable role in transforming the entire paradigm of commerce and selling and purchasing of the products and services. In particular, it can be stated that the innovative and advanced technological tools have fostered the notion of electronic transactions or simply electronic commerce (e-commerce). Electronic commerce is nothing more the approach that encompasses the activities of performing business activities, electronically. It has been documented in the studies of [12] that electronic commerce is primarily based on the electronic processing and data transmission, which may include video, sound, and text. In order to support this idea, [25] has stated that electronic commerce or electronic transactions include several different activities. These activities may include after-sales service, direct consumer marketing, public procurement, online sourcing, collaborative engineering and design, commercial auctions, electronic bills of lading, electronic share trading, electronic fund transfers, digital content's online delivery, and electronic trading of services and goods [18]. It is important to note that electronic transactions may encompass both services (for instance, legal, financial, and information services) and products (for instance, specialized equipment, consumer goods), as well as the traditional activities.

It has been established that electronic transactions mainly include commercial transactions that are usually supported by the closed and open networked communication and information systems. These communication and information systems are connected with efficient software and computers that are usually used to foster the transmission of data. Although, these platforms play an appreciable role in smooth and hassle free transactions, but these platforms also increases the risk of security attacks [27]. Since, these platforms offers direct interface amid the internet and users, it eventually increases certain threats to the privacy of customer's confidential information. The analysis of the study of [16] has presented an idea that when a customer performs transaction on any website or online platform, the backlog of the entire activity is automatically generated in the system. This backlog incorporates all information about the confidential and private information of the customers, like name, browsing history, address, credit card information. It has been analyzed that this information is utilized by the businesses to understand the demands of the customers to improve their products and services [10]. However, if the information systems or IT network infrastructure of an organization is targeted by the hackers, it may also cause severe damages to the integrity of customer's information. In typical electronic transaction environment, the payee, payer, as well as the financial institution, as shown in figure 1. Under this hierarchy, the customers have to exchange or share their information with the company, so as to complete the transaction. It is observed that this structure usually increases the threat of security breaches and other malicious activities. In this regard, [12] has stated that such situations usually result in identity theft, credit card frauds, fake financial transactions that ultimately results in irreversible harm to the customers as well as to the company, in terms of loss of repute. Therefore, it can be affirmed that electronic transactions is one of the greatest threats for the information and privacy of the customers [20].

Figure 1: Characteristic Scenario in Electronic Transactions

3.2 Self –Regulation Approach

Self-regulation can be understood as the regulatory process in which an industry level company enforces and sets standards and rules, related to the organizational conduct within the industry [13]. One of the notable aspects of self-regulation is that it is entirely different from the government level regulations. It has been recognized that businesses usually makes use of this approach in order to minimize certain potential risks and vulnerabilities that may affect the repute of the organization. In accordance with the study of [24] businesses have started to develop and implement self-regulation to avoid the threat of excessive regulations of the government. In some areas of the businesses, there is not any proper government regulation that could ensure the integrity of the business. In such circumstances, businesses usually prefer to develop their own regulations [22], so as to ascertain risk free operations. It has been examined from the analysis of different researches that enforcing and monitoring regulations are one of the most imperative aspects of the regulatory process [21]. However, self-regulation utilizes the approach of self-policing as the prime mechanism, in order to assure compliance while providing remediation.

3.3 Self-Regulation in Electronic Transactions

It has been observed in the study of [18] that initially the e-commerce sector adopted pure enforcement and pure market models to safeguard the confidentiality and privacy of customer's information. Unfortunately, both of these models got fail, as they did not reach and fulfill the desired requirements of privacy protection. On the other hand, the approach of self-regulation is found to provide higher levels of privacy and security to the confidential information of the customers, without affecting the budgetary conditions. When self-regulation is used to safeguard the information and privacy of the customers, in electronic environment, it can be occurred in three traditional components. These conventional components of power include adjudication, enforcement, as well as legislation [13]. In this regard, the study of [20] has presented an idea about legislation, which shows that this component mainly relates to the question that who should demonstrate adequate rules for privacy protection. On the other hand, enforcement is found to be related to the question that defines that who is responsible for initiating the actions of enforcing privacy legislations. Besides that, adjudication defines who should decide and evaluate the potential violation of the security rules [25].

All of these components of the self-regulation approach enable the companies and industries, specifically electronic commerce sector, to develop appropriate rules and legislations in order to secure the information of their client from malicious activities. It is significant to bring into the notice that self-regulation appreciably supports the electronic commerce industry, as compared to the conventional governmental standards and regulations. It is due to the fact that it enables the industry to develop their laws and regulations, according to the need of privacy, instead of following the general governmental regulations [17]. Within the electronic commerce industry, a number of self-regulations are being developed and used, in terms of development of organization based IT policies, deployment of certain standards, integration of verification methods, and data security standards. All of these initiatives solely intend to protect the integrity and confidentiality of the information and privacy of the customers, while enabling them to perform electronic transactions.

3.4 Fundamentals of Effective Self-Regulation to Safeguard the Information and Privacy of the Customers

The study of [8] shows that e-commerce sector is continually striving to develop consumer-friendly, meaningful, and fruitful self-regulatory regimes in order to protect their privacy of their business processes and customer's information. However, it is important to note that to be fruitful, self-regulation should do more than the articulate guidelines or policies. It is integral to note that effective and efficient self-regulation includes substantive means and rules to assure that customers also understand the rules that are developed by the company [7]. This approach plays an incredible role in improving and enhancing the overall security and privacy of customer's data [26]. It is because; this feature also enables the users to properly complying with the self-regulatory regimes that are developed by the industry. The proceeding research encapsulates the analysis brief analysis of the fundamentals of effective self-regulation that are crucial for the appropriate and foolproof protection of customer's privacy. One of the most fundamental elements of effective self-regulation for the protection of privacy includes fair information practices [23]. Fair information practices encompass various features including access of consumers to their identifiable data, appropriate security levels, choice, and awareness of customers about the regime [1].

In the context of awareness, it is observed that customers usually do not know about the identity of a person that collects their personal information. It is a fact that electronic transactions are fully automated in nature, but to some extent the consumers have to manually share their personal information with the e-commerce company [9]. It has been established that such situations increases privacy related risks. In terms of choice, companies must ensure to provide an open choice to their customers about the utilization of their personal information. In other words, e-commerce companies should provide an opportunity to their client to exercise choice, in terms of how and whether their personal information is utilized, either by business or by third party vendors [18]. Moreover, it is also essential for the development of the effective self-regulatory regimes that customers are provided with the facility to access their desired information, so that they can amend and correct their information. Data security also holds undeniable significance in the development of effective self-regulatory rules. It also includes the assurance of the protection level at the extended levels [5]. Privacy policies hold integral position in the self-regulatory rules, as it covers all aspects of the internal and external operations of the organization. The privacy policies play a commendable role in protecting the confidentiality and integrity of data, without intruding electronic transaction activities.

3.5 Importance of Self-Regulation in Electronic Transactions to Protect Customer Information and Privacy

Self-regulation can be considered as one of the most appropriate approaches that ensures the reliability of electronic transactions. It has been stated by [24] that self-regulation is more pertinent and credible than government regulations. It is due to the fact that government regulations are usually developed in the generalized manner, while considering the highlighted issues of the particular industry. On the other hand, self-regulatory rules are developed for

particular industry, while profoundly assessing its issues and potential risks [3] In terms of securing the private data of the customers, during electronic transactions, self-regulatory regimes enable the customers to properly understand that how they are supposed to exchange their data with the company. This feature ultimately helps the companies in reducing the risk of potential vulnerabilities, like security breaches, data theft, identity theft of the client, fraudulent transactions [26].

On contrary to the government regulations, self-regulations foster more effective and faster remediation, enforcement, monitoring, and rulemaking processes that ultimately results in the fruitful outcomes [6]. In addition to this, it has also been established that self-regulation also plays an incredible role in increasing the flexibility for the consumers and businesses, as it clearly elaborates all essential guidelines, crucial for the data protection. This feature also allows the industry to minimize their compliance expenditures, while increasing overall efficacy. It has been suggested in the research work of [5] that because of having uncountable benefits, industry self-regulation of the security and privacy of consumer data has been considered as the most flexible alternative to the conventional government regulations, specifically in the perspective of electronic transactions.

4 Discussion and Analysis

The emergence of electronic commerce or remote purchasing trends has played a major role in bringing ease and convenience for the consumers as well as for the business. However, electronic transactions have also increased the liability to the businesses towards the protection of their customer's data and ensuring their privacy. It has been established from the study of [15] that during incidents of security breaches and data theft are continually increasing, specifically in the area of electronic transactions. In this regard, recent statistical data is also presented in below mentioned figure 2.

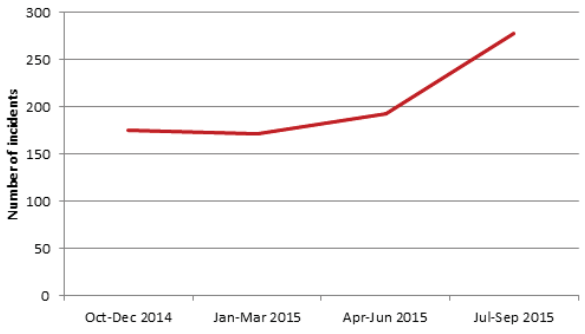

Figure 2: Graphical Representation of the Security Issues related to Electronic Transactions

Above mentioned graph clearly depicts the idea that the information of the customers, performing electronic transactions, is at high risk of exposure or misuse. Figure 3 shows that remote purchase or fake transactions are the most prevalent threat in e-commerce industry [11]. During the year 2004, the total percentage for fraudulent transactions was approximately 30 percent. However, in the year 2014, it was eventually increased up to 69 percent, which shows that the situation has become graver; thereby, needs to have more cohesive strategies or approaches to combat this issue and safeguard the information of the customers as well as their privacy [6].

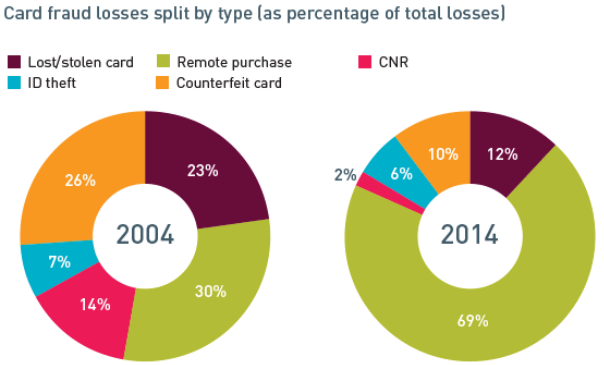

Figure 3: Diagram showing Statistics of Fraudulent Transactions due to the Weak Security of Customer's Information

In such circumstances, self-regulation can be considered as the most optimal solution to the problem. In electronic transactions, self-regulatory regimes or rules help in safeguarding the confidentiality and privacy of the customers. A self-regulatory security regime incorporates such mechanisms and features that ensure the strict compliance with the rules [16]. In addition to this, the approach also presents an opportunity to the affected party to immediately cope with the issue, even when the predefined rules are not appropriately followed. In accordance with the study of [16], self-regulation presents wide range of benefits to the e-commerce sector, particularly in the context of secured and highly protected electronic transactions. This approach allows the concerned authorities to develop such security rules and policies that ultimately secure the private information of the consumers, while providing hassle free access to the authorized personnel [4]. One of the most commendable aspects of self-regulation, in safe electronic transactions is that the approach mainly works on the ethical values and norms. In other words, it can be stated that the self-regulatory rules mainly focuses on the role of the profession or industry in enforcing and creating norms of behavior [2]. It depicts such idea that makes individual feel ethical constraints against exploiting the integrity of the personal information of the customers; hence, protecting the privacy of the customers, also from internal threats.

5 Conclusion

The preceding research has incorporated the profound assessment of the importance of self-regulation in electronic transactions, particularly to safeguard customer information and privacy. After the accomplishment of this research, it has been established that the protection of customer's information has become the greatest concern for the businesses, due to the transference of information through electronic transactions. Currently, businesses have started to put especial emphasis on the establishment of self-regulatory regimes, in order to ascertain the integrity of their client's data. Analysis shows that self-regulation is more effective and flexible, as compared to traditional governmental regulations. It is because; self-regulatory rules are especially designed after assessing the needs of the specific industry or users. This research work has presented the in-depth analysis of the importance of self-regulation in electronic transaction to protect customer's information. Moreover, customers will be now putting up extra trust on their vendors regarding the online transactions. Fact of the matter is that, with growing technologies and their implementation, there are various pros and cons that come into existence. Information travelling and e-transactions have highly facilitated users, though data security and privacy has been a point of concern. New issues arise and are subjected to be addressed by new solutions. Incorporation of technologies for ensuring data privacy and security, considering its significance has been drastically taken a good face, due to the fact of electronic transactions being a growing medium.

6 References

[1]. Adelola, T., Dawson, R. and Batmaz, F., 2014, December. Privacy and data protection in E-commerce: The effectiveness of a government regulation approach in developing nations, using Nigeria as a case. In Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for (pp. 234-239). IEEE.

[2]. Almunawar, M.N. Securing Electronic Transactions to Support E-Commerce. arXiv preprint arXiv: 1207.4292 (2012)

[3]. Brennan, M., 2013. Managing Risk and Ensuring Quality: Nova Scotia's Framework for Regulatory Excellence. Journal of Nursing Regulation, 4(2), pp.39-42.

[4]. Chhagan, M., Kauchali, S. and Van den Broeck, J., 2013. The Data Management Plan. In Epidemiology: Principles and Practical Guidelines (pp. 261-279). Springer Netherlands.

[5]. Ciocchetti, C. A. E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. American Business Law Journal, 44(1), 55-126. (2007)

[6]. Dilling, O., 2012. From compliance to rulemaking: how global corporate norms emerge from interplay with states and stakeholders. German LJ, 13, p.III.

[7]. Djelassi, S. and Decoopman, I., 2013. Customers' participation in product development through crowdsourcing: Issues and implications. Industrial Marketing Management, 42(5), pp.683-692.

[8]. Ezzi, S.W., 2014. A theoretical Model for Internet banking: beyond perceived usefulness and ease of use. Archives of Business Research, 2(2), pp.31-46.

[9]. Fang, Y., Qureshi, I., Sun, H., McCole, P., Ramsey, E. and Lim, K.H., 2014. Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-Commerce Institutional Mechanisms. Mis Quarterly, 38(2), pp.407-427.

[10]. Gebauer, H., Paiola, M. and Saccani, N., 2013. Characterizing service networks for moving from products to solutions. Industrial Marketing Management, 42(1), pp.31-46.

[11]. Gu, J. and Huang, S., 2014. Countermeasures of Coping With Lacking of Credibility in E-commerce Under the Background of the International Crisis. Contemporary Logistics, (16), p.49.

[12]. Hu, Y. J., & Tang, Z. Protecting Online Privacy: Self-Regulation, Mandatory Standards, or Caveat Emptor Zhulei Tang. In in Proceedings of the Fourth Annual Workshop on Economics and Information Security. (2005)

[13]. Jarupunphol, P., & Buathong, W. Secure Electronic Transactions (SET): A Case of Secure System Project Failures. Transactions, 16, 22 (2013)

[14]. Jayabalan, S., Commerce and Consumer Protection: The Importance of Legislative Measures (2012)

[15]. King, N.J. and Raja, V.T., 2012. Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), pp.308-319.

[16]. Listokin, S.B, 2015. Industry Self-Regulation of Data Privacy and Security.SSRN (2015)

[17]. Morris, B.W., Kleist, V.F., Dull, R.B. and Tanner, C.D., 2014. Secure information market: A model to support information sharing, data fusion, privacy, and decisions. Journal of Information Systems, 28(1), pp.269-285.

[18]. Murphy, M.M. Privacy Protection for Customer Financial Information, Congressional Research Service. (2014)

[19]. Niranjanamurthy, M. and Chahar, D.D., 2013. The study of e-commerce security issues and solutions. International Journal of Advanced Research in Computer and Communication Engineering, 2(7), pp.2885-2895.

[20]. Niranjanamurthy, M., and Dr Dharmendra C. The study of e-commerce security issues and solutions.

International Journal of Advanced Research in Computer and Communication Engineering 2, no. 7. (2013)

[21]. Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Fischer-Hubner, S., Millard, C., Lotz, V., Jaatun, M.G. and Leenes, R., 2012, December. Accountability for cloud and other future internet services. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on (pp. 629-632). IEEE.

[22]. Peltier, T.R., 2013. Information security fundamentals. CRC Press.

[23]. Schwaig, K.S., Segars, A.H., Grover, V. and Fiedler, K.D., 2013. A model of consumers' perceptions of the invasion of information privacy. Information & Management, 50(1), pp.1-12.

[24]. Singh, A., and Karan S. A review: secure payment system for electronic transaction. International Journal of Advanced Research in Computer Science and Software Engineering (JARCSSE) 2. (2012)

[25]. Smith, H. J., Dinev, T., & Xu, H. Information privacy research: an interdisciplinary review. MIS quarterly, 35(4), 989-1016. (2011)

[26]. Tang, Z., Hu, Y., & Smith, M. D. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. Journal of Management Information Systems, 24(4), 153-173. (2008)

[27]. Turban, E., King, D., Lee, J.K., Liang, T.P. and Turban, D.C., 2015. E-Commerce Security and Fraud Issues and Protections. In Electronic Commerce (pp. 457-518). Springer International Publishing.

[28]. Zimmermann, S. and Rentrop, C., 2014. On the Emergence of Shadow IT-A Transaction Cost-Based Approach.

DR. IBRAHEEM MUBARAK ALHARBI is Assistant Professor, Head of Management Information Systems Department in College of Business at University of Jeddah, Saudi Arabia. He received a PhD from School of Business at La Trobe University. He is membership of ACS since 2008, publishes widely including journal articles, and he regularly presents his research at international academic conferences. His academic information systems research interests include business and online transactions, security and information privacy, electronic commerce, and knowledge Management Systems. imalharbi@uj.edu.sa

DR. BADER ABDULRAHMAN ALYOUBI is Assistant Professor, Department of Management Information Systems in the College of Business at the University of Jeddah, Saudi Arabia. He received his PhD from the Department of Information Science at King Abdulaziz University in Jeddah, in the Specialization (knowledge management), including published widely journal articles, he regularly presents his research in international academic conferences. His research interests include academic information systems, knowledge management systems and commercial transactions on the Internet, and information security and privacy, e-commerce, and decision support systems knowledge perspective. balyoubi@uj.edu.sa