EasyChair Preprint

№ 2180

E-Commerce interfering with Privacy: Perceived Risks and Security issues with Techno-policy outcomes

Avinash Singh

December 16, 2019

E-Commerce interfering with Privacy: Perceived Risks and Security issues with Techno-policy outcomes

1- Introduction: Privacy and E-commerce

Privacy is being an issue that concerns citizens of countries with normality attained governmental setup (unlike countries dealing with civil unrest and unstable or failed governments) and said privacy is likely to be floundered with e-presence of individuals on many online platforms that seek to develop and monitor behavioural attributes of user's life with the help of its e-working on the multiple platforms. Precisely defining privacy is difficult as it embodies multitoned features of civil and political rights along with social, economic and cultural concerns, however in context to e-space, we can rely of definition illustrated by *Lee A. Bygrave* of Norwegian Research Centre for Computers and Law, University of Oslo who defines privacy as "a condition or state in which a person(Or organization) is more or less inaccessible to others, either on spatial, psychological or informational plane"[1] which explains the extent of privacy in subjective contexts of its existence. Privacy with the alignment to the individual's prerogative harvests with the legal protection and socio-legal attributes that are majorly connected with the freedom and choice of life that needs to be unmingled without slightest external interferences or unwarranted observance. In present paper, privacy risks are associated with the e-commerce platforms and by the time we attain an unfettered check over privacy violations or third-party control on these e-commerce entities, there should be a decisive movement prolonged towards securing the possible means to curb the privacy violations.

It is very likely that the privacy could be subjective or context driven which could be put in the words as "contextual integrity" and what information is shared (appropriateness) with reference to a context and how far the revelation of such consumer data is streamed (flow or distribution) in a context could be a defining line for privacy[2], especially when privacy seems

[1] Bygrave, L. A. (2001). Electronic agents and privacy: A cyberspace odyssey 2001.*International Journal of Law and Information Technology, 9*(3), 275-294(279). doi:10.1093/ijlit/9.3.275

[2] Bargh, M. S., Choenni, S., & Meijer, R. (2017). On addressing privacy in disseminating judicial data: Towards a methodology. *Transforming Government: People, Process and Policy, 11*(1), 9-41(17). doi:http://dx.doi.org/10.1108/TG-12-2015-0051

to be intertwined with the transparency.[3] India has also witnessed a growth in said e-commerce industry as appropriately observed in research *Mahipal and other*[4] wherein online commerce have been divided into two phases with the first phase being advent of B2B directory, recruitment and marital platforms launched between 1996 to 2005 and post 2005 witnessed the presence of online travel bookings for all modes of transport starting with air travel. In the second phase itself, the group purchasing websites have launched that have given birth to present form of the e-commerce retail industry that is still developing and expanding in both horizontal and vertical segment of market with around 36% of Compound Annual Growth Rate till 2016.[5]

With many subjective sectors influencing the privacy and its subsets, we chose to develop our exploratory dialect within the e-commerce platforms that serves the purpose of easiness of market access through internet, and with all possible means, in a lucrative deal offering the attention of buyers present online. The user or customer at e-commerce platform provide explicit and implicit information about themselves while using the e-shopping platform[6] that raises concerns about sharing such data in an unauthorized manner leading to privacy rights violation, which in turn are not shared might lead to profit revenue generation in long run through e-trust creation[7] as discussed later. This could be observed in cases of explicitly providing preference information like product rating, comment and purchase details while implicit user preferences are also drawn through monitoring viewing time, search performed or saved items for future buying and springing to external websites from e-shopping portal. Also, transactional information such as payment mode and details in case of e-banking are gathered by e-commerce while also collecting explicit identification information such as name, address and other such personal details while implicitly providing identification details such as IP address.

---

[4]Mahipal, D., & Shankaraiah, K. (2018). E-COMMERCE GROWTH IN INDIA: A STUDY OF SEGMENTS CONTRIBUTION. *Academy of Marketing Studies Journal, 22*(2), 1-10(2-3). Retrieved from https://search.proquest.com/docview/2123609133?accountid=44542

[5] Id. at p.6.

[6] Ben Schafer, J., Konstan, J. A., & Riedl, J. (2001). E-commerce recommendation applications. *Data Mining and Knowledge Discovery, 5*(1-2), 115-153(148). doi:http://dx.doi.org/10.1023/A:1009804230409

[7] Mandic, M. (2009). Privatnost I Sigurnost U Elektronickom Poslovanju/Privacy And Security In E-Commerce. *Trziste = Market, 21*(2), 247-260(252). Retrieved from https://search.proquest.com/docview/229994042?accountid=44542

There are two major issues that are prima facie drawn out of privacy protection of netizens wherein first issue relates to the access to the consumer data and information by the online platforms and secondly is the misuse of the data by the agencies in possession of such data.[8] With the fuzzier lining drawn between the offline and online transactions[9], it is pertinent to settle the behavioural targeting is no less far away than opted on the whims of the companies delivering the product to their customers. Security/Privacy issues are very adaptable to the satisfaction corelative as they have high impact on the online shopping experience of the customers[10] and hence significance is proven to be of great importance in present context of e-commerce transactions, though in few researches like one by *Tianxiang Sheng* & *Chunlin Liu* who concludes a less significance impact of privacy adoption to the customer satisfaction while showing an higher effect on customer loyalty[11], but the issue in present is to derive the right based approach to them rather than dwelling into managerial and economic perspective. However, privacy is corelated with the security, however a reedy distinction could be drawn out of the two that is to say an information is secure when owner of the information have control over it whereas, privacy belongs when subject of the information have control over its usage albeit requires security to act over it.[12]

User privacy protection towards lawful accessing the platforms is one of the critical issue that effectually builds trust among customers and e-commerce portals, thus moving towards a confident browsing/transactional attitude.[13] With the traditional organizations using their

[8] Al Abri, D., McGill, T., & Dixon, M. (2009). Examining the impact of E-privacy risk concerns on citizens' intentions to use E-government services: An oman perspective. *Journal of Information Privacy & Security, 5*(2), 3-26. Retrieved from https://search.proquest.com/docview/203668879?accountid=44542

[9] Frederik, J. Z. B. (2015), Infra n. 52 at p. 164.

[10] Liu, X., He, M., Gao, F., & Xie, P. (2008). An empirical study of online shopping customer satisfaction in china: A holistic perspective. *International Journal of Retail & Distribution Management, 36*(11), 919-940(930). doi:http://dx.doi.org/10.1108/09590550810911683

[11] Sheng, T., & Liu, C. (2010). An empirical study on the effect of e-service quality on online customer satisfaction and loyalty. *Nankai Business Review International, 1*(3), 273-283(279). doi:http://dx.doi.org/10.1108/20408741011069205

[12] Coursaris, C., Hassanein, K., & Head, M. (2003). M-commerce in canada: An interaction framework for wireless privacy. *Canadian Journal of Administrative Sciences, 20*(1), 54-73. Retrieved from https://search.proquest.com/docview/204876154?accountid=44542

[13] Ayoade, J. O., & Kosuge, T. (2002), Infra n. 79 at p. 287.

websites for e-commerce purpose[14], it is apparent that in coming days there would be a complete of e-commercialization of present material market as we see in today, and hence the privacy concerns are to be increased multi-fold in imminent period of time. However, e-commerce with a wide distinctiveness comparatively form the traditional commerce, with more automated, impersonal, fewer direct interaction, with higher legal qualms and more chances of fraud and manipulation[15] unquestionably generates need of structuring e-commerce platform highly monitored and duly watched for privacy checks.

2- Behavioural aspect: Struggling Privacy within e-commerce industry

The start of the behaviour mapping could be deduced from a very interesting perspective that relates to the digital mapping which in recent years have drawn much noise in the e-industry. Google maps being the forerunner with its service "street view" have attracted the concern of a UK based attorney Mark Watts, which in his scholarly work have seen an analysis on its effect on the EU Directives that includes Directive on e-privacy and directive on data protection which doesn't clarifies the situation on digital mapping.[16] A complex issue is dealt in form of WiFi Mapping that includes Network Data and Approximate Location Data, now with the EU Directive in place, restraining the geographical data collection that falls under the purview of EU Directive on e-privacy which include location as *"any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service"*[17] and also restraining the 'personal data' that includes the data of identifiable or identified individual which in words of directive be delivered by meaning as "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or

[14] Ladson, A., & Fraunholz, B. (2005). Facilitating online privacy on eCommerce websites: An australian experience. *Journal of Information, Communication and Ethics in Society, 3*(2), 59-68. doi:10.1108/14779960580000261

[15] Bojang, I. (2017). Determinants of Trust in B2c E-Commerce And Their Relationship With Consumer Online Trust: A Case Of Ekaterinburg, Russian Federation. *Journal of Internet Banking and Commerce, 22*, 1-59. Retrieved from https://search.proquest.com/docview/1932307529?accountid=44542

[16] Watts, M., Brunger, J., & Shires, K. (2011). Do european data protection laws apply to the collection of WiFi network data for use in geolocation look-up services? *International Data Privacy Law, 1*(3), 149-160. doi:http://dx.doi.org/10.1093/idpl/ipr013

[17] European Parliament and of the Council, Directive 2002/58/EC *Official Journal L 201 , 31/07/2002 P. 0037 – 0047.*

social identity"[18] There are other facets of the behavioural mapping based on which the companies tries to access the nature of consumer response while interacting with the websites that includes privacy attitude, privacy belief, information sensitivity, privacy social norm.[19] Now, as it is assiduously argued and explored that the privacy could be on threat with the WiFi Mapping while providing distinction between mapping a 'source' and an 'individual' while observing that an extensive interpretation of the personal data could have 'far-reaching and undesirable consequences'[20].

However, said issue have lightened over privacy and e-commerce data intake as it could be hazardous to the whole idea of privacy protection, which if broadly analysed, will present an alternative threat of, what is called as "Behaviour Mapping" that is a classic approach to control an individual's daily business by infiltrating into the e-social life knowing the preferences. Moreover, it raises deep concerns over the economic leverage that these e-commerce platforms help to gains to the third party websites, which when in receipt of user data, use them to present lucratively to the target audience which potentially shadows the reality among the consumers, which wouldn't be so abysmal in absence of such consumer data. Also, there are consumer data threat dependent on the type of the information and these risk are very peculiar when they are used by the interested party, like disclosure of name has lower risk than that of the credit card information[21] which makes the e-commerce platforms more vulnerable as they intake all sort of personal data during end user consumer interface on their platform. One of the major e-commerce hub Amazon collects data from their customers that based upon their previous shopping and website browsing pattern shows items list visiting the next time that could potentially be of interests to the recurring customer, however, no data selling observed in recent studies by amazon.com which only shares such data with

[18] The European Parliament And Of The Council, Directive 95/46/EC, *Official Journal L 281 , 23/11/1995 P. 0031 – 0050.*

[19] Infra n. at p. 27. < Xu, H. (2009). Consumer responses to the introduction of privacy protection measures: An exploratory research framework. *International Journal of E-Business Research, 5*(2), 21-47. Retrieved from https://search.proquest.com/docview/222254670?accountid=44542>

[20] Supra n. at p. 158< Watts, M., Brunger, J., & Shires, K. (2011). Do european data protection laws apply to the collection of WiFi network data for use in geolocation look-up services? *International Data Privacy Law, 1*(3), 149-160. doi:http://dx.doi.org/10.1093/idpl/ipr013>

[21] Stephen, C. R. (2017). What's your anonymity worth? establishing a marketplace for the valuation and control of individuals' anonymity and personal data. *Digital Policy, Regulation and Governance, 19*(5), 353-366(359). doi:http://dx.doi.org/10.1108/DPRG-05-2017-0018

the subsidiary owned by them.[22] However, discussions in later part of the paper will prove to be more inclined towards continued practise of privacy right violation of customers by marketers[23] as observed in other researches.

It is noteworthy that the online businesses need the customer shopping preferences and emotional and feeling related metrics to comprehensively determine the value and potential of a customer that leads to limit the success or failure intensity in e-commerce platforms[24], however, said behavioural mapping have clear potential to damagingly touch upon the issue. Demographics have been the ley reliant feature that the e-commerce platforms have monitored and with the perception shift in adult customers using the e-commerce platforms relying on the e-payments with increasing trust and awareness assured by banking industry[25] have given boom to the sector, nonetheless older customers are traced to be more privacy defensive than younger one in a recent study[26], henceforth businesses should ensure incidents related to unauthorized data access and privacy concerns of the said age group, which includes children as will having more than million in number with handy access of internet[27] and their personal data collection is perceived as a very serious privacy issue for their parents.[28] Such demographical shift could lead to risking the newly earning class and e-commerce players are trying to capture the next-gen customers[29] with strong grip over their preferences, thus making a competitive marketing strategy, which in present case is

[22] Farah, B. N., & Higby, M. A. (2001). E-commerce and privacy: Conflict and opportunity. *Journal of Education for Business, 76*(6), 303-307(304). Retrieved from https://search.proquest.com/docview/202819391?accountid=44542

[23] Ibid.

[24] Schaupp, L. C., & Bélanger, F. (2005). A CONJOINT ANALYSIS OF ONLINE CONSUMER SATISFACTION1. *Journal of Electronic Commerce Research, 6*(2), 95-111. Retrieved from https://search.proquest.com/docview/236648456?accountid=44542

[25] Dixit, N., M.B.A., & Datta, S. K. (2010). Acceptance of E-banking among adult customers: An empirical investigation in india. *Journal of Internet Banking and Commerce, 15*(2), 1-17(5). Retrieved from https://search.proquest.com/docview/763169929?accountid=44542

[26]Madden, G., Banerjee, A., Rappoport, P. N., & Suenaga, H. (2017). E-commerce transactions, the installed base of credit cards, and the potential mobile E-commerce adoption. *Applied Economics, 49*(1), 21-32(25). doi:10.1080/00036846.2016.1189507

[27] Liu, C., & Arnett, K. P. (2002). An examination of privacy policies in fortune 500 web sites. *Mid - American Journal of Business, 17*(1), 13-21(18). Retrieved from https://search.proquest.com/docview/214179301?accountid=44542

[28] Karakaya, F., & Charlton, E. T. (2001). Electronic commerce: Current and future practices. *Managerial Finance, 27*(7), 42-53(45). Retrieved from https://search.proquest.com/docview/212664330?accountid=44542

[29] Maleki, M., & Pasha, M. A. (2012), Infra n. 66 at p. 12.

behavioural mapping to which consent cannot be attained even if the child as a customer gives express consent thereto as has not attained the legal age to give consent while many children give away the information because online shopping is 'cool and natural' for them irrespective of awareness about security and reliability of e-commerce platforms.[30] Trans-geographical study towards Indian and US citizens have also found a set of behavioural perception that hinders sharing of information form Indian side of participants than compared with US side based on the differences in individualism and power distance relationship among the US and Indian customers wherein Indian customers are more cautious of entities and less likely to build trust outside extended family and friends.[31]

Although, studies have also shown in countries like Malaysia[32] that the age and educational status have not impacted the e-commerce related banking rather the user interface leading to accessibility in e-commerce platforms have greater impact on e-commerce business, but that couldn't be the benchmark to follow considering the variation in geographical and behavioural attitude of customers around globe. In fact researches have spotted the usage behaviour of the customer on e-commerce platforms that seemed to be dependent upon the "choice" of disclosing personal information given to them.[33] Trust and confidence are direct participants in e-commerce industry and could be invariably defined in simple phrase presented by *Antoniou & Betten* is "trustor's expectation about motives and behaviour of trustee's"[34], hence, another demographic characteristic that stimulates behavioural response of trust towards e-commerce market is the cultural trend of economies impacting the confidence on e-commerce transactions. Like in country of France, having lower trust culture, portrays significantly lower confidence in e-commerce transactions as opposed to

---

[30] Clarke, J. "Children and E-commerce: Challenges and Opportunities." And G. Salvendy, and M. J. Smith. "Systems, Social and Internationalization." *Design Aspects of Human-Computer Interaction.* New Orleans: Routledge, (2001): 541-543.

[31] Infra n. at p. 44. < Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). FACILITATING GLOBAL E-COMMERCE: A COMPARISON OF CONSUMERS' WILLINGNESS TO DISCLOSE PERSONAL INFORMATION ONLINE IN THE U.S. AND IN INDIA.*Journal of Electronic Commerce Research, 11*(1), 41-52. Retrieved from https://search.proquest.com/docview/236644862?accountid=44542>

[32] Sohail, M, and Shanmugham, B. (2004). E-banking and Customers' preferences in Malaysia: an empirical investigation. *Information sciences, Informatics and Computer Science: an International journal, 150 (3-4),* 207-217.

[33] Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users. *Information Technology & People, 28*(3), 426-441(431). doi:http://dx.doi.org/10.1108/ITP-10-2014-0232

[34] Antoniou, G., & Batten, L. (2011). E-commerce: Protecting purchaser privacy to enforce trust. *Electronic Commerce Research, 11*(4), 421-456(422). doi:http://dx.doi.org/10.1007/s10660-011-9083-3

country such as Germany with high-trust society exhibiting higher confidence in conducting e-commerce[35], thus it could be concluded that the privacy concerns are inversely proportion to shopping the decision of the customer at e-commerce platform[36] and could pursue customers to provide incomplete & false information on websites asking for such personal information.[37]

E-commerce services stretching from retail to service sector have created an new risk zone in behavioural mapping where not only personal details are the root subjects of privacy invasion, rather, the services relating to legal compliance and registrations also put their respective client at risk when these services are provided by online platforms[38], which is followed by medical and financial services offered on the e-business platform that gathers vital information from customers having potential of its malicious use risking to social and economic loss[39], while also making it easier to target the weak point of the victim for privacy invasion. Studies have also mapped the behaviour of customers in terms of purchasing that is inclined towards lowering graph considering an outweighing of the risk perceptions over ease of access and usage of an e-commerce portal.[40]

3- Banking Industry: Close alley to e-commerce

Banking industry being the most common ally in privacy protection framework for the e-commerce websites has appropriately impacted the customer perception in dealing with the e-commerce website, also, providing base to the ease of access that have driven influx in e-marketing in contemporary era. Security and privacy related policy, more than the ease of

---

[35] Desai, M. S., Desai, K. J., & Phelps, L. D. (2012). E-commerce policies and customer privacy: A longitudinal study (2000-2010). *Information Management & Computer Security, 20*(3), 222-244(225). doi:http://dx.doi.org/10.1108/09685221211247325

[36] Gajendra, S., & Wang, L. (2014). Ethical perspectives on e-commerce: An empirical investigation. *Internet Research, 24*(4), 414-435(418). doi:http://dx.doi.org/10.1108/IntR-07-2013-0162

[37] Gupta, B., Iyer, L. S., & Weisskirch, R. S. (2010). Facilitating Global E-Commerce: A Comparison Of Consumers' Willingness To Disclose Personal Information Online In The U.S. And In India. *Journal of Electronic Commerce Research, 11*(1), 41-52(42). Retrieved from https://search.proquest.com/docview/236644862?accountid=44542

[38] Helms, G. I., & Mancino, J. M. (1999). Information technology issues for the attest, audit, and assurance services functions. *The CPA Journal, 69*(5), 62-63(63). Retrieved from https://search.proquest.com/docview/212260473?accountid=44542

[39] Sharma, S., & Toshniwal, D. (2017). Scalable two-phase co-occurring sensitive pattern hiding using MapReduce. *Journal of Big Data, 4*(1), 1-18(2). doi:http://dx.doi.org/10.1186/s40537-017-0064-9

[40] Featherman, M. S., & Hajli, N. (2016). Self-service technologies and e-services risks in social commerce era. *Journal of Business Ethics, 139*(2), 251-269(257). doi:http://dx.doi.org/10.1007/s10551-015-2614-4

access, have shaped the customer adoption towards online banking[41], and such privacy and security related policy working towards consumers personal and financial protection could attract more traffic onto the e-commerce platforms.[42] Security of transaction and availability of modes of payment, that are mostly banking related functions, act as catalyst for consumer satisfaction at e-commerce platform.[43] With the e-banking system having a lower transactional cost, the banks seems to prefer and develop it for the future, meanwhile attaining a competitive advantage, however, there were problems faced by such banking companies that count in the minimal customer response and design and implementation of design of security systems, which was primarily a problem faced by banks in Greece.[44] It could be highly useful to compare it with the Indian scenario with the lower familiarity of technologically advanced devices among the common public (especially in rural areas), which in turn risk the privacy of customers who opt for using such e-banking channel as mode of transaction at e-commerce websites. This could be one of the berries that e-commerce companies have synthesized as potential perils and mooted the 'Cash on Delivery' as mode of payment, but this couldn't hinder the ever-growing access and adoption of e-payment channels.

Even at the global level, the privacy concerns are plaguing the electronic payment systems among other factors[45] that initiated an ongoing research & global dialogue in recent years, wherein e-commerce firms inherit concerns about the privacy issues of the electronic payment systems provided by banks and hence it contributes to form trust perception and concentration of usage by the firms as concluded in a study[46] with sample population form country Malaysia. However, Malaysia is still stands on better footing than the country

[41] Hua, G., PhD. (2009). An experimental investigation of online banking adoption in china. *Journal of Internet Banking and Commerce, 14*(1), 1-12. Retrieved from https://search.proquest.com/docview/231969736?accountid=44542

[42] Id at p. 10.

[43] Maria Delarosa, D. D., & Sahid, S. N. (2013). The antecedents of online customer satisfaction and customer loyalty. *Journal of Business and Retail Management Research, 07*(2), 1-12(5). Retrieved from https://search.proquest.com/docview/1700402511?accountid=44542

[44] Angelakopoulos, G., & Mihiotis, A. (2011). E-banking: Challenges and opportunities in the greek banking sector. *Electronic Commerce Research, 11*(3), 297-319(317). doi:http://dx.doi.org/10.1007/s10660-011-9076-2

[45] Harris, H., Guru, B. K., & Avvari, M. V. (2011). Evidence of firms' perceptions toward electronic payment systems (EPS) in malaysia. *International Journal of Business and Information, 6*(2), 226-245(233). Retrieved from https://search.proquest.com/docview/910985658?accountid=44542

[46] Id at p. 241.

Vietnam as part of ASEAN group, wherein the government ruling over many business transaction and unclear laws on online banking have created security and privacy concerns among the users of e-commerce in the country, howsoever the Vietnamese Government believe the potential of e-commerce for economic growth of the country[47], it is still an infrastructural challenge for online banking industry that is deeply connected to the e-commerce industry.

4- Challenges

Concerns have been deeply observed towards perception based perils, which in general, are rooted among the users of the services creating a trust issue in alliance with effective usage preferences for the ongoing e-activities, wherein a study for the Oman region has showed a lowering tendencies to use the e-government services remaining the privacy concerns whereas such will be uncalled for a government to move with digitalized functioning that creates the e-privacy perception positively impacting the perceived trustworthiness and usefulness of e-government services.[48]

E-service development is one of the key focus of the governments in the past, and it is more likely to be regulated on an outset, but the e-commerce websites that attracts a large e-traffic with a multitude of possible privacy outbreaks could also create an adverse impact on the e-governmental services in a region, which should be carefully analysed while observing the intensity of effective peril occurring stretch of e-privacy concerns on e-commerce platforms. Data breaches due to internal control issue among e-commerce houses and in few cases intentional privacy outbreak by e-business websites flouting their own explicit privacy policy posed a great deal of threat to their customers[49], hence consumer privacy risk can be reduced by their perceived ability to control of information being collected and usage of such information data.[50]However, it is noted in various researches that intangibility of e-commerce business has foremost effect on perceived risk among consumers in form of psychological

[47] Chong, A. Y., Keng-Boon Ooi, Lin, B., & Tan, B. (2010). Online banking adoption: An empirical analysis. *The International Journal of Bank Marketing, 28*(4), 267-287(271). doi:http://dx.doi.org/10.1108/02652321011054963

[48] Al Abri, D., McGill, T., & Dixon, M. (2009), Supra n. 8.

[49] Moscove, S. A. (2001). E-business security and controls. *The CPA Journal, 71*(11), 40-46(46). Retrieved from https://search.proquest.com/docview/212302561?accountid=44542

[50] Bandyopadhyay, S. (2011). Online privacy concerns of indian consumers. *The International Business & Economics Research Journal, 10*(2), 93-100(94). Retrieved from https://search.proquest.com/docview/856122021?accountid=44542

risk, performance risk, social risk etc.[51] that are directly related to the privacy and security concerns of an individual.

The data that is to be gathered must have following attributes i.e. (i) freely given, (ii) specific, (iii) informed (iv) indication of wishes, by which the data subject signifies agreement to his or her personal data being processed as per the Article 2(h) of the EU Data Protection Directive. One of the major apprehensions lies in the proximity of the real obeisance of such attributes as there are no benchmark or assurances that could ensure the compliance of stringent 'consent check' and hence the potential fragility in this 'data game' is higher than it guises. However, it was observed that the e-privacy directive and data protection directive still lacks a synchronization that needs to be fixed, for example, e-privacy directive deals with the legal persons as well, while there are no protection granted for the legal persons in data protection directive.[52] Also, law seemed to be weakly focused at global level in case of e-transactions where the new "who is on the other side" i.e. payment intermediaries or "electronic agents" whose role is ambiguous and thus the legal scope ability of contractual relationship of electronic agents [53] seemed to be globally neglected or progressing with slow pace which could be a big challenge for e-commerce domain whose blood and vein of business are e-payment channels and the ultimate fatalities lies their customers and their e-privacy rights, while the legal way out could be mandatory privacy/security breach notification, like in the State of California in USA and other such regulations mad part of EU discussion on privacy protection[54], but the state of issue lies still far away from appropriate protection.

One other such international issue, though restricted analytically to US, has been raised through a research on the bankrupt companies that have filed for insolvencies and are on the verge of selling their asset that in few cases include the customer identification data which is point of sale in such transaction. Leaving the technicality aside, the behaviour of such companies has been determined through reading their privacy policy where in some cases it

[51] Marcelo, V. N., Laroche, M., Marie-Odile, R., & Eggert, A. (2012). Relationship between intangibility and perceived risk: Moderating effect of privacy, system security and general security concerns. *The Journal of Consumer Marketing, 29*(3), 176-189(178). doi:http://dx.doi.org/10.1108/07363761211221701

[52]Frederik, J. Z. B. (2015). Personal data processing for behavioural targeting: Which legal basis? *International Data Privacy Law, 5*(3), 163-176(173). doi:http://dx.doi.org/10.1093/idpl/ipv011

[53] Quirk, P. (2008;2007;). Curriculum themes: Teaching global cyberlaw. *International Journal of Law and Information Technology, 16*(3), 297-308(301). doi:10.1093/ijlit/ean006

[54] Id. at p. 307.

was objected by the state department as illegal to sell the data. Other big e-commerce companies have later adopted a privacy policy that protects them from such threat of state department's intervention as they asked for consent in their privacy policy for disclosure and selling of personal identifiable data collected on their website. This could be into a foggy situation between establishing an ecosystem of trust and confidence among customers while also leveraging as much as possible for a company to use such data in a flexible and permissible manner.[55]

In very few cases consumers are aware of their privacy rights, though being actively concerned about their privacy[56], lack the understanding of the e-portal they are accessing into, and hence, human readable privacy policies and access to privacy seals are very necessary steps that the e-commerce websites have deliberately left unexploited, like one of the very early trust seal named as "WebTrust" that used independent verification to prevent online fraud and privacy infringement.[57] However, arguments have been made in response to the privacy seals utility wherein they were claimed potentially deceptive, as only acting as legal compliance and not retracting away the privacy concerns from the web portals.[58] Consumer awareness towards the e-privacy rights and all their concerns (could reach as an 'obsession' in case of a study done for US citizens) could even be an unreliable factor at the stage of assessing their usage behaviour for such e-commerce platforms[59], which makes the behavioural attribute as indeterminant based upon the individuals preferences according to time, requirement and functional environment, yet significant, when studied from point view of data collection by e-commerce platforms for behavioural mapping as matter of privacy transgression that also affects the risk perception[60] among other factors like trust and security.

---

[55] Carroll, B. (2002). Price of privacy: Selling consumer databases in bankruptcy.*Journal of Interactive Marketing, 16*(3), 47-58(56). Retrieved from https://search.proquest.com/docview/229609238?accountid=44542

[56] Beatty, P., Reay, I., Dick, S., & Miller, J. (2007). P3P adoption on E-commerce web sites: A survey and analysis. *IEEE Internet Computing, 11*(2), 65-71(67). doi:10.1109/MIC.2007.45

[57] Pugliese, A. J., & Halse, R. (2000). SysTrust and WebTrust: Technology assurance opportunities. *The CPA Journal, 70*(11), 28-34(32). Retrieved from https://search.proquest.com/docview/212308582?accountid=44542

[58] Rodrigues, R., Wright, D., & Wadhwa, K. (2013). Developing a privacy seal scheme (that works). *International Data Privacy Law, 3*(2), 100-116(106). doi:http://dx.doi.org/10.1093/idpl/ips037

[59] Desai, M. S., Richards, T. C., & Desai, K. J. (2003). E-commerce policies and customer privacy. *Information Management & Computer Security, 11*(1), 19-27(20). Retrieved from https://search.proquest.com/docview/212367253?accountid=44542

[60] Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security, 24*(4), 348-371(352). doi:http://dx.doi.org/10.1108/ICS-05-2015-0020

It is very well observed by *Someshwar Kesh* and others in his work on e-commerce security that dictates the interlinked security related traits that include application development platforms, database management, system software and network infrastructure as significant for the appreciable functioning of e-commerce with customer privacy compliance, though there is a red flag inherited into it as failure or weakness of one of the key traits could lead in system failure as jeopardising security[61] that breaks privacy insulation. With the merging of consumer data at the internally and at different supply chain of product in e-commerce, the challenge to maintain data privacy is getting harder[62] and standard managerial practises needs to be advanced to survive the data outflow risking customers privacy.

E-businesses across the internet have opted for e-assurances like privacy seals, trust certificates , third party endorsements and even the money back guarantee etc. varying across the segment of the market ranging from their monetary value[63], but there remains a key concerns relating to the small e-commerce businesses that lack the basic infrastructure of gaining access to the trust assurances (that are easily accessible to comparatively large e-commerce platforms) or other such new layer of security measures that comes with a corresponding cost[64], which in turn creates an anti-competitive regime, thus presenting challenge in form of infrastructural dearth in the e-commerce sector with economic & legal standpoint, while also routing customer data exclusively to few large e-commerce houses, which in turn have greater leverage to utilize such data to create a near monopolistic control over market. In anti-competitive context, findings of *John-ren Chen & Christian Smekal* seems upon touching the issue as they at first perceive e-commerce as equalizer to the international trade barrier but looking upon the infrastructurally and technologically scarce countries, to them that are developing countries, worsens the "digital dividend" at

[61] Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. *Information Management & Computer Security, 10*(4), 149-158. Retrieved from https://search.proquest.com/docview/212327693?accountid=44542

[62] Liu, C., & Arnett, K. P. (2002). Raising a red flag on global WWW privacy policies. *The Journal of Computer Information Systems, 43*(1), 117-127(118). Retrieved from https://search.proquest.com/docview/232575331?accountid=44542

[63] Karimov, F. P., & Brengman, M. (2014). An examination of trust assurances adopted by top internet retailers: Unveiling some critical determinants.*Electronic Commerce Research, 14*(4), 459-496. doi:http://dx.doi.org/10.1007/s10660-014-9148-1

[64] Guynes, C. S., Wu, Y. '., & Windsor, J. (2011). E-Commerce/Network security considerations. *International Journal of Management and Information Systems, 15*(2), 1-7(6). Retrieved from https://search.proquest.com/docview/864899620?accountid=44542

international forum[65] which strongly implicates an unobserved and unattended anti-competitive practise at international level.

Comprehensive profiling of the customers or "web roamers"[66] and their short-term relationship with the e-commerce portals have measured challenges of data abundancy, of which utilization could be made perilously by the e-commerce platform for unwarranted interference through hitting very cornerstone of human freedom i.e. privacy. In addition to data abundancy, the are severe and unrelenting delinquencies continue towards the privacy infringement in e-commerce world with rapid change in technologies and entrance of new systems and technological tools in market[67] that makes hackers and pro-privacy fissure entities one step ahead of privacy minders, because it shouldn't be left unrecalled that merging of IT with Communication Technologies moving towards the network computing is the base model over which today's e-commerce stands.[68]

M-commerce have also flourished to possess an extended thereat to the privacy of individual, and because of its augmented identity tracking capabilities, there are severe risks associated with it while using it for e-commerce from mobile that becomes m-commerce. Unlike normal e-commerce that collects data as IP Address which usually changes from time, the mobile data contains location and other such details which could be used by e-commerce websites for extended data collection compared to stationary e-commerce.[69] Therefore it could be concluded that m-commerce is an extension of the stationary e-commerce, however unique in its extent to provide more detailed identifying data line IMEI Number, Device Serial Number, Location details, Sim ID and other such specifications to the online commercial

---

[65] Chen, J., & Smekal, C. (2009). Should the WTO deal with e-trade taxation issues?*Progress in Development Studies*, *9*(4), 339-348(340). doi:http://dx.doi.org/10.1177/146499340900900407

[66] Maleki, M., & Pasha, M. A. (2012). Ethical challenges: Customers' rights. *SCMS Journal of Indian Management*, *9*(4), 5-21(7). Retrieved from https://search.proquest.com/docview/1536049344?accountid=44542

[67] Tran, E., & Atkinson, M. (2002). Security of personal data across national borders. *Information Management & Computer Security*, *10*(5), 237-241(237). Retrieved from https://search.proquest.com/docview/212302912?accountid=44542

[68] The business case for electronic commerce. (1999). *International Journal of Retail & Distribution Management*, *27*(11), 464-465(464). Retrieved from https://search.proquest.com/docview/210947123?accountid=44542

[69] Zhang, R., Chen, J. Q., & Lee, C. J. (2013). MOBILE COMMERCE AND CONSUMER PRIVACY CONCERNS. *The Journal of Computer Information Systems*, *53*(4), 31-38(34). Retrieved from https://search.proquest.com/docview/1429691269?accountid=44542

hubs, which in turn result in targeted advertising and solicitation offers which is repetitive infringement of privacy rights.[70]

5- Regulatory Regime and Security Shields

It is pertinent to draw a distinction between the regulatory regime and the core legal provisioning that covers the data protection and e-privacy of the citizens. Unlike the Cape Verde constitution that originated in 1980 and later being re-constituted in 1992, with a substantial amendment in 1999, is a young piece of legal document as compared to the Indian counterpart that has seen no drastic changes for the field of e-world. Example of Cape Verde is essential in present context, as the government there have recognized the near necessity and significance of data protection and privacy rights along with other substitutes and implanted the same in the constitution itself. However, more important the fact is that the data protection and privacy rights are very observantly protected through, not just constitutional tools, but also making a strategic policy towards the telecommunication laws and EU based data protection regime that includes Data protection and E-privacy related directives[71] in the overall framework of privacy right protection. In present context, Iran had floated a legislative regime namely Electronic Commerce Law in 2004, wherein data privacy protection regulations are treasured to provide an explicit privacy protection at e-commerce platform, along with other legislative protection in form of penal and civil laws working for such privacy protection[72], which certainty shows a greater concern for citizens privacy at the country's governmental regime. However, it may not be possible to regulate the specifics of the privacy protection in the e-commerce world as access to it is through internet which is still the ungoverned realm[73], to which making a law at a geographical basis would be just moderately addressing the issue of privacy which is still left unclear of its regulatory approach over other countries.

---

[70] *Id.* at p. 37.

[71] Traça, J. L., & Embry, B. (2011). An overview of the legal regime for data protection in cape verde. *International Data Privacy Law*, 1(4), 249-255. doi:http://dx.doi.org/10.1093/idpl/ipr017

[72] Hassan, K. H., & Bagheri, P. (2016), Infra n. 86 at p. 5.

[73] Fasli, M. (2007). On agent technology for e-commerce: Trust, security and legal issues. *The Knowledge Engineering Review, 22*(1), 3-35(25). doi:http://dx.doi.org/10.1017/S0269888907001014

Thus, the issue raises a pertinent stake in the long run when the privacy rights and user data, that are generally taken in a "non-unequivocal" consensus from the customer on the e-commerce platforms, about the privacy and data protection of customers served by the e-commerce platforms. It is also important for the regulatory point of view to look into the system of operational structure being followed in the country of which uncertainty would have effect on the consumer privacy wherein like in case of cookie management, country like UK have based its approach on acceptance of opt-out system to obtain consent for cookies whereas in case of the Netherlands that requires the indication of wishes for the valid consent. Also, countries like Germany and Canada along with UK have made privacy protection regulation in form of legislations that seek to regulate collection, use and transfer of personal information, including transfer of data to the foreign land depending upon the privacy regulation existing in the respective country[74] like transfer of personal data as per the EU Directive on data Protection is explicitly barred that is envisioned for transmission to countries lacking "adequate" data protection.[75] However, outcome of Safe Harbour Principle after long-drawn-out negotiations between USA and EU have given hope and suggestive structure of data transfer among the respective region[76] but such a move is still awaited in other nations evidencing boom in e-commerce industry where need for data and privacy safety at global level is warranted.

It is observed that the science, technology and society have a close tie up with relative influences on each other thus marking a "contextual interaction" and hence the social and political system has bi-folded impact on innovation which in turn diffuses with the social system and increasing its value with the adopters of such innovation.[77] Thus the advent of e-commerce as an innovation diffused with the cultural mix of the society have administered the development of regulatory framework in various countries and hence multinational e-

[74] Boritz, J. E., & No, W. G. (2011). Infra n. 106 at p. 16.

[75] Sheldon, L. A., & Strader, T. J. (2002). Managerial issues for expanding into international web-based electronic commerce. *S.A.M.Advanced Management Journal, 67*(3), 22-30(29). Retrieved from https://search.proquest.com/docview/231143332?accountid=44542

[76] Yonge, W., & Massey, R. (2007). The distance marketing of financial services -- A UK overview. *Journal of Financial Services Marketing, 11*(4), 370-380(378). doi:http://dx.doi.org/10.1057/palgrave.fsm.4760053

[77] Rudraswamy, V., & Vance, D. A. (2001). Transborder data flows: Adoption and diffusion of protective legislation in the global electronic commerce environment. *Logistics Information Management, 14*(1), 127-136(133). Retrieved from https://search.proquest.com/docview/220028606?accountid=44542

commerce platforms are faced to protect privacy in the global e-commerce market with higher individual concern for individual security.

Scholars have placed the privacy and security as the non-technical limitation to the e-commerce business[78] which seems to be measurably flawed at very outset because of the nature of business conducted in the e-space which itself is a technology at broad level. Privacy and security could only be approached for its regulation if they originally dawn in the first place that is because of technological influx to retail business, therefore, privacy may originally be a subset of non-technical limitation due to an element of customer's behaviour and attitude infusion, but e-privacy is a widely held and separate dimension while dealing with e-commerce industry containing incidental subjective traits to be analysed in due course. Data security has key main features that are needed to be addressed in an environment of common, yet crucial attributes taken into consideration i.e. availability, confidentiality, integrity and usage.[79] Regulation mooted in Singapore have been driven by the ever expanding e-commerce industry and consumer confidence, though they have errantly neglected the spirit of defending the rights of the data subject, rather, were based on the economic considerations that involves thriving data storage and processing industry in the country.[80] Alongside the regulatory approach towards protecting privacy, the contribution of stakeholders through self-regulation could be an useful tool in protecting the electronic privacy of personal information[81] like one in the country of America that formerly continued on the boulevard of aspiration towards pro-deregulation regime.[82] Large e-commerce companies could take a step forward towards securing the e-privacy along the industry independent of the regulatory approach that may come in form of technological or research

[78] Tara, F. H., & Mahboob, R. (2008). E-commerce in bahrain: The non-technical limitations. *Education, Business and Society: Contemporary Middle Eastern Issues, 1*(3), 213-220(216). doi:http://dx.doi.org/10.1108/17537980810909832

[79] Ayoade, J. O., & Kosuge, T. (2002). Breakthrough in privacy concerns and lawful access conflicts. *Telematics and Informatics, 19*(4), 273-289(275). doi:10.1016/S0736-5853(01)00017-X

[80] Chesterman, S. (2012). AFTER PRIVACY: THE RISE OF FACEBOOK, THE FALL OF WIKILEAKS, AND SINGAPORE'S PERSONAL DATA PROTECTION ACT 2012.*Singapore Journal of Legal Studies*,391-415(414). Retrieved from https://search.proquest.com/docview/1380879789?accountid=44542

[81] Xu, H. (2009). Consumer responses to the introduction of privacy protection measures: An exploratory research framework. *International Journal of E-Business Research, 5*(2), 21-47(24). Retrieved from https://search.proquest.com/docview/222254670?accountid=44542

[82] Wijnholds,Heiko de B.and Michael W.Little. (2001). Regulatory issues for global E-tailers: Marketing implications. *Academy of Marketing Science Review, 2001,* 1-12(2). Retrieved from https://search.proquest.com/docview/200836942?accountid=44542

support for the whole industry. This could even be made part of the charity work or corporate social responsibility which will help to save and nourish privacy fortification in e-business society.

On the security side of the privacy protection, there have been a distinction being made between the snoopers and hackers, wherein the former has a legit access to the data of an organization as they have to sophisticatedly analysis the e-commerce database and thus the inferential disclosure (identity and value disclosure) and security seemed as challenging issue to resolve[83], to which a security alternative in form of data perturbation offered encryption in form of noise term that masks the original attributes from the snoopers thus giving them perturbed values.[84] Therefore, privacy as a barrier to e-commerce[85] in form of user data when camouflaged with false consumer data will distort the impetus of potential perils revolving around e-commerce sector. Technology is significant enabler in data protection in e-space as it builds trust in the e-commerce transactions by way of creating data protection regime for sustainable growth meeting the pace of online space.[86] This could be witnessed by a study on e-commerce in pharmaceutical sector that exhibited strong barriers such as technological support and privacy issues among others towards advancing perceptible growth in adoption and usage[87] which speaks about the relevancy of technologically related support and development needed in the e-commerce industry as a whole. There has been a security addendum at the transaction level of the e-commerce in form of shared PIN verification/usage that could lead to the privacy protection at certain level while observing

[83] Muralidhar, K., Sarathy, R., & Parsa, R. (2001). An improved security requirement for data perturbation with implications for e-commerce.*Decision Sciences, 32*(4), 683-698(684). Retrieved from https://search.proquest.com/docview/198081415?accountid=44542

[84] Id. at p. 685.

[85] Singh, N., Yadav, M., & Sahu, O. (2016). Consumer acceptance of apparel e-commerce–Ethiopia. *Intelektine Ekonomika, 10*(1) Retrieved from https://search.proquest.com/docview/2006835526?accountid=44542

[86] Hassan, K. H., & Bagheri, P. (2016). Data privacy in electronic commerce: Analysing legal provisions in iran. *Journal of Internet Banking and Commerce, 21*(1), 1-14. Retrieved from https://search.proquest.com/docview/1799378205?accountid=44542

[87] Zanamwe, N., Bere, M., Zungura, C., Muchangani, B., & Nyamakura, S. A. (2012). E-Commerce Usage In The Pharmaceutical Sector Of Zimbabwe. *Journal of Internet Banking and Commerce, 17*(1), 1-15(11). Retrieved from https://search.proquest.com/docview/1016751442?accountid=44542

the consensus of the customer at several levels[88] (to which end PIN verification must be made available at such levels).

Howsoever the attempts being made by the technological advancements, the externalities in form of hacker couldn't be sorted out yet, and comparatively low-cost entry, absence of spatial boundaries and legal weakness or absenteeism nurtures favourable environment for hackers to attack the e-commerce websites[89] that eventually put customer at menace of privacy hazards.

6- Suggestive Remarks

The internet handling technologies have gone far ahead of securing the privacy towards the end user with the advent of its counter perils and hence the Privacy Enhancing Technologies have been developed in the context of the end user usage to prevent any misuse of data, in which regard, the P3P technologies of which adoption by the e-commerce websites is very low than expected, and with the study indicating a less than 10% combined adoption rate as per the data of e-commerce top 300, Forbes, ranking.com in year 2007[90] which is apparently approximate to the 2003 study on same subject by AT& T Survey. However, there are key drivers indicating a positive trend in adoption of the P3P technology as an PET compliance of that could be enlisted as legislative compliances, potential brand image stability that could be harmed due to privacy breach and data management[91], though the case in back 2000's was disastrous, as companies have lost sight over the challenge that the customer privacy could lead towards their business advancement.[92] Studies in 2010 have also concluded that privacy as 'satisfier' doesn't impact negatively to the customer if poorly performed by the e-commerce hubs, however, are positively perceived if privacy protection is complied by the e-

[88] Tang, J., Terziyan, V., & Veijalainen, J. (2003). Distributed PIN verification scheme for improving security of mobile devices. *Mobile Networks and Applications, 8*(2), 159-175(173). Retrieved from https://search.proquest.com/docview/205055345?accountid=44542

[89] McCrohan, K. F. (2003). Facing the threats to electronic commerce. *The Journal of Business & Industrial Marketing, 18*(2), 133-143(139). Retrieved from https://search.proquest.com/docview/221997422?accountid=44542

[90] Beatty, P., Reay, I., Dick, S., & Miller, J. (2007), Supra n. 56 at 67.

[91] Karat, C. Brodie, C. and Karat, J. (2003) Views of Privacy: Business Drivers, Strategy, and Directions, tech. report, *IBM Research*. Retrieved at http://domino.research.ibm.com/library/ cyberdig.nsf/1e4115aea78b6e7c85256b360066f0d4/06f417 65cbd41f4285256db8004ae7e3?OpenDocument.

[92] Fink, J., & Kobsa, A. (2000). A review and analysis of commercial user modeling servers for personalization on the world wide web. *User Modeling and User - Adapted Interaction, 10*(2-3), 209-249(230). Retrieved from https://search.proquest.com/docview/212958027?accountid=44542

commerce platforms[93], which in consistent terms seems facilely inappropriate, and thus could be cagey to make such claim in 2018 as the present policy and awareness have gone far ahead with the mushrooming e-stores and media attention to the issue of the privacy, that in turn being responded in good terms by non-visitation behaviour on e-commerce websites to which customers they are not familiar with.[94] However awareness about the existence of such e-commerce platform is as important for customers as it is to educate them about the security and privacy challenges that are potentially faced by them while using the web which not only increase the importance of web assurances security seals[95], but also make them overall expedient in exploring the new safety horizons that could help them to prevent any possible privacy transgression on e-commerce websites.

Privacy issues in the near future have a greater impact on the buying pattern of the customers, and as earlier described as challenge for lack of infrastructural support, all the e-commerce platforms must be provide with the basic and effective privacy protection infra and standardized privacy policy by the regulatory authorities, and with the booming sector of the e-commerce at individual level wherein home made products are being sold by the families, including the growing local food and beverage industry, the need for such infrastructural support would be imminently warranted as essential feature of the core national policy and budgetary documents. This is high time think for the Small Scale Enterprises to mark their presence on e-business market, with the higher access of internet and increased online purchasing by businesses (in B2B segment), and also, slow but consistent growth, in B2C segment would open new doors for SME's in e-commerce scattered economy based on relationship, network and information.[96] Increased use of e-commerce have gained momentum to flourish the SME's with a cost effectiveness, interoperability, interactivity &

[93] Ramanathan, R. (2010). E-commerce success criteria: Determining which criteria count most. *Electronic Commerce Research, 10*(2), 191-208(205). doi:http://dx.doi.org/10.1007/s10660-010-9051-3

[94] Kim, S. H., & Byramjee, F. (2014). Effects of risks on online consumers' purchasing behavior: Are they risk-averse or risk-taking? *Journal of Applied Business Research, 30*(1), 161-n/a. Retrieved from https://search.proquest.com/docview/1500357183?accountid=44542

[95] Mascha, M. F., Miller, C. L., & Janvrin, D. J. (2011). The effect of encryption on internet purchase intent in multiple vendor and product risk settings.*Electronic Commerce Research, 11*(4), 401-419(416). doi:http://dx.doi.org/10.1007/s10660-011-9080-6

[96] Peterson, D., Meinert, D., Criswell, J.,II, & Crossland, M. (2007). Consumer trust: Privacy policies and third-party seals. *Journal of Small Business and Enterprise Development, 14*(4), 654-669(655). doi:http://dx.doi.org/10.1108/14626000710832758

scalability traits[97], while also presents challenges towards increased infrastructural cost[98] in form of hardware and software installation as the increased intensity of consumer comparison with that of competitors.

We can offer the though, that the privacy may not be the determinant factor towards building the trust as the customers are more aware of the security than of privacy, however it is still the benchmark to conclude that the customers perception towards bank's ability for securing their personal information and transaction on e-commerce platform is the key determinant of the e-privacy in digital era.[99] However, in recent researches carried with the same subject matter relating to the privacy and e-commerce business functioning, it has been clearly visible that privacy as one of the key dimension of the e-service quality have a positive impact on the customer value satisfaction in terms social, functional and economic value side, and hence, it subsequently affects the customer satisfaction and loyalty towards the e-commerce platforms[100], which demonstrates the essence of privacy protection from a business point of view as well, remaining the erstwhile legal significance intact. Privacy thus could eb protected by either building a trust perception among customers towards the e-markets by efforts of the e-commerce entities or another way out as suggested by *Rhys Smith & Jianhua Shao* is that technological alternatives towards the privacy compliance must be made mandatory for the e-commerce entities to follow or to say that "forcefully" implementing protection regime for respecting privacy rights of the customer through technological tolls.[101] Privacy as determinant feature of the service quality while using the system to access the e-commerce platform have a positive impact on the service quality perception among the consumers and hence e-commerce platforms are direct stakeholders in privacy compliance while the system operators like in present case the mobile companies are

---

[97] Rayport, J.E. and Jaworski, B.J. (2001), E-commerce, McGraw Hill Higher Education, New York, NY, pp. 86-96.

[98] Asghar, A. J., Zhang, S. X., & Brem, A. (2013). E-commerce for SMEs: Empirical insights from three countries. *Journal of Small Business and Enterprise Development, 20*(4), 849-865(850). Retrieved from https://search.proquest.com/docview/1462472707?accountid=44542

[99] Dixit, N., M.B.A., & Datta, S. K. (2010). Supra n. 25 at p.13.

[100] Bressolles, G., Durrieu, F., & Deans, K. R. (2015). An examination of the online service-profit chain. *International Journal of Retail & Distribution Management, 43*(8), 727-751(742). doi:http://dx.doi.org/10.1108/IJRDM-11-2013-0214

[101] Smith, R., & Shao, J. (2007). Privacy and e-commerce: A consumer-centric perspective. *Electronic Commerce Research, 7*(2), 89-116(90). doi:http://dx.doi.org/10.1007/s10660-007-9002-9

also the incidental, yet essential, stakeholders in forming behavioural intention of consumers.[102]

Privacy not only is enshrines at the national level, rather, it is much regarded phenomenon at the international trade arena wherein protecting privacy gains confidence in e-commerce that is placed at par importance with lifting up the trade barriers at international level[103], also, in the wake of US exiting form Trans-Pacific Partnership had one of the major goals of setting up international standards for e-commerce platforms[104] among others. US regulation as approved by the Federal trace Commission (FTC) could be a guiding light for privacy guardians with the self-regulation being recognized as passive means to protect privacy and sole measure for consumer transactions with the e-commerce.[105] There must be a global initiative to initiate a research colloquy among the researchers of Management Information System and Audit Information System[106] along with Legal & Policy Thinktanks so as to widen the reach and development of e-privacy protection regime at global level and sharing such development to the countries lacking such technological capabilities at time, adding to which, technological advents in fields of data analytics could also be deployed other than traditional approaches to data mining[107] to innocuously defend the privacy concerns at the individual level. Along with research advents to protect privacy, there could be a mandatory ethics officer[108] appointed in the e-commerce companies that would be appointed through external sources and have authority to check the privacy compliance in the e-commerce

[102]Vlachos, P. A., & Vrechopoulos, A. P. (2008). Determinants of behavioral intentions in the mobile internet services market. *The Journal of Services Marketing, 22*(4), 280-291(289). doi:http://dx.doi.org/10.1108/08876040810881687

[103] Huang, J. (2017). Comparison of E-commerce regulations in chinese and american FTAs: Converging approaches, diverging contents, and polycentric directions? *Netherlands International Law Review, 64*(2), 309-337(321). doi:http://dx.doi.org/10.1007/s40802-017-0094-1

[104] id at p. 310.

[105] Shimanek, A. E. (2001). Do you want milk with those cookies?: Complying with the safe harbor privacy principles. *Journal of Corporation Law, 26*(2), 455-477(476). Retrieved from https://search.proquest.com/docview/220757299?accountid=44542

[106] Boritz, J. E., & No, W. G. (2011). E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems, 25*(2), 11-45(12). Retrieved from https://search.proquest.com/docview/1034564474?accountid=44542

[107] P Ram, M. R., Krishna, S. M., & Siva Kumar, ,A.P. (2018). Privacy preservation techniques in big data analytics: A survey. *Journal of Big Data, 5*(1), 1-12(9). doi:http://dx.doi.org/10.1186/s40537-018-0141-8

[108] Peeples, D. K. (2002). Instilling consumer confidence in e-commerce.*S.A.M.Advanced Management Journal, 67*(4), 26-31(29). Retrieved from https://search.proquest.com/docview/231254603?accountid=44542

company. These external ethics officers must be made legislatively protected and regulated in a manner to be most transparent and accountable to the privacy and security acquiescence, which in turn would act as catalyst towards building trust among the customers. Scaling attempts with variations in terms of purpose, context, dimensions etc. factors like IUIPC (Internet User Information Privacy Concern), GIPC (Global Information Privacy Concern) or CFIP (Concern for Information Privacy) have evolved over time through matrices and quantifiable data research[109] that have developed the need to provide systematic control over privacy and data sharing in the concurrent e-space of their time.

It is acceptable norm that here might not be an absolute privacy attainable as the risk of surrendering certain degree of information (that indeed are sometimes necessary for internet access)[110] that would always be worthier of risk taken in disclosing such personal information. On the contrary, consumer behaviour assessed based on the potential assumptions about the future action of the vendor, response to which in several researches, have established as deeply flawed in such instances of consumer behaviour.[111] Henceforth, the only possible conclusion that could be drawn is that whatever may be the regulatory and socio-economic shields to protect e-privacy, the risk of human 'need-based attitude' wouldn't be altered and always be used by the e-businesses to target them, and not to disregard that, after all of such behavioural mapping done till date, this is at least these e-businesses houses would have already predicted. We are always at risk of a brisk adversity in e-privacy commotions to which a regular subjective and objective reality check would provide an armour against heavily populated e-business houses among others in the future.

[109] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model.*Information Systems Research, 15*(4), 336-355(340). Retrieved from https://search.proquest.com/docview/208156803?accountid=44542

[110] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61-80,100. Retrieved from https://search.proquest.com/docview/208156649?accountid=44542

[111] Reay, I., Beatty, P., Dick, S., & Miller, J. (2009). Do you know where your data is? A study of the effect of enforcement strategies on privacy policies. *International Journal of Information Security and Privacy (IJISP), 3*(4), 68-95(70). doi:10.4018/jisp.2009100105