



ORIGINAL CONTRIBUTION

## Privacy of Internet Users in the Era of Transformative Marketing

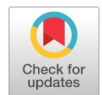
Muhammad Farooq<sup>1\*</sup>, Qasim Ali Qureshi<sup>2</sup>

<sup>1</sup> Limkokwing University of Creative Technology, Cyberjaya, Malaysia

<sup>2</sup> Universiti Utara Malaysia, Changlun, Malaysia

**Abstract**— Advancement in technology has connected the world. It has made life more comfortable. Today we can order any product from all over the world with just one click using e-commerce sites like Amazon and Alibaba. These developments have led to transformative marketing. This exponential increase in internet usage and growth in e-commerce companies has created numerous opportunities for both users and companies. However, as the internet grew, businesses worldwide started collecting customer's data to very minute details. As per business organizations, customer data is collected to serve customers in a better way. Although it is not impossible, yet it is difficult for an e-commerce company to process transaction of a customer without asking his/her name, the address of delivery and payment mode. Customers all over the world have concerns over sharing their information. 'companies have applied different security procedures to resolve customer's concerns, which assure that customer data is not leaked or used in unethical business activity. Privacy is the primary concern of internet users all over the world. Therefore, this research article addresses the customer concern of privacy over the internet pertaining to e-commerce companies in the era of transformative marketing. The paper discusses different drivers and challenges of customer's data protection. The article also explores the two prominent prospects on Internet privacy; the "Consumer protection view" and "free-market view". The researchers advocate the consumer protection view. The consumers must have control over privacy and sharing of their content. If they feel secure to share their information, there should be an option for the consumers to allow the sharing of consumer information. Secondly, the government's compliance is also important. The companies should also allow consumers to revoke their shared information whenever they feel insecure. It will give confidence to the consumers to work with the company, and companies will also have loyal customers.

**Index Terms**— Customer Privacy, Internet Users, E-commerce, Consumer Protection View, Free-market View, Transformative Marketing.



**Received:** 23 March 2020; **Accepted:** 11 October 2020; **Published:** 19 December 2020

### Introduction

Technology has revolutionized the world (Argyriou et al., 2006; Jain & Aggarwal, 2015; Johnson, 2017; Ramaiyah & Ahmad, 2010). It has changed all of life, education (Farooq, Rehman, et al., 2019), telecommunication (Farooq & Raju, 2019), transportation (Farooq, Muhammad, et al., 2019), banking (Farooq, Kalimuthu, & Reza, 2019) and even religious practices (Farooq et al., 2018). All these changes in several sectors came due to information system (Basu, 2009; Enck et al., 2014; Lowry et al., 2017). In an information system, the core product is Privacy (Boritz et al., 2008; Schae-witz et al., 2020; Su et al., 2005; Zhou et al., 2010). Despite the increase in internet penetration and development of IOT and internet products, there has been least focus on user privacy protection (Aichholzer & Strauß, 2010; Cachin, 1997; Deng et al., 2011; Klewitz-Hommelsen, 2002; Spiek-ermann & Cranor, 2009; Roy et al., 2010; Zhou et al., 2010). Therefore, this paper views the possible options for user privacy concerns.

Privacy is referred to as the capability of an individual or group to isolate them physically and their information. Privacy also means a speciality

of information or commodity to other people or groups. Therefore, the security of it at the individual and group level is essential. Privacy keeps the integrity of humans, individuals, and governments. Thus privacy and security are key agreements expected from the consumer for subscribing to a service or using a product. Privacy and security impact performance and growth aspects of individuals and groups with the advancement in communication (Schae-witz et al., 2020; Jacobsson et al., 2016).

To maintain privacy, citizens across the world have different types of rights. Since the earlier times, individuals and groups have right to be alone, the right to have limited access to resources without providing their information, the right to control information, the right to stay in a state of privacy, the right to keep secrecy, right of personhood and autonomy, right to have self-identity, personal growth, and intimacy (Knijnenburg et al., 2013). However, all these aspects have changed after the development of the internet. With the introduction of the World Wide Web, the privacy of the user started becoming limited. The World Wide Web requires information from the user. Internet needs actions from users, which reduces their privacy. Information shared by users on several social platforms

\*Email: farooq.buzdar2@gmail.com

and other platforms is analysed to extract insights. The aggregation of information and conclusion further breach consumer privacy. With the advancement in internet, the users started looking for a new definition of privacy. Recently privacy has been defined as

*"The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, property, thoughts, feelings, secrets, and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner, and timing of the use of those parts we choose to disclose"* (Spiekermann & Cranor, 2009).

In the business world, before availing and subscribing to any information, users are shared a privacy agreement. In privacy agreement, users agree to share their information in return for using a product or service. For the sharing of information, there are two types of privacy viewpoints. The first is "Consumer protection view" and the second is "free-market view." Same two prominent approaches are used in customer's data sharing in online environment. The viewpoint of the market approach, in which a user decides the flow of the data, the users have to agree to provide information. If information is provided, the user does not know where information will be used. The free-market approach definition is as per the guidelines of Organisation for Economic Co-operation and Development "OECD", The free market is also verified by General Data Protection Regulation "GDPR" and European Union. Contrary to that, there is an approach of consumer protection view. This approach has been derived from the customer rights movement. In this approach, it is said that individuals may not have the time and knowledge to evaluate every resource. The individuals may not even track the recorded information. In support of this viewpoint, Jensen and Potts showed and proved that most of the users don't understand privacy laws and agreements made by organizations and governments.

## Methodology

In this article, a review of literature on privacy from a transformative marketing point of view is made. It was reviewed how users are managing their privacy in the era of transformative marketing. A review was made of recent articles published in high-quality journals relevant to the topic.

First the term privacy was clarified in terms of its definition. Then the reason for less development of frameworks and models on consumer privacy issues is stated. The literature on studies done on privacy concern from the point of view of business consumers as well as public organizations such as hospitals are shared. The effect of privacy concern on hospital selection is shared. Studies on social media users are analyzed. Then study on privacy in time of crisis is reviewed. Another area focused is the value of consumer data to organizations, as well as areas that organizations need to focus on gaining consumer trust. A study on user privacy preferences, as well as the effect of age, is also reviewed. Type of privacy and its applicability to online business is reviewed. Conflicting theories on privacy are shared. Lastly, studies on large multinational companies are shared, and then a conclusion is made.

## Literature Review

In years to come, the internet of things will open several possibilities in communication and lifestyle improvement. However it will also bring new privacy dilemmas. The focus on privacy in last 10 years has been very little, which led to the development of fewer frameworks and fewer models on Mobile Users' Information Privacy Concerns (MUIPC). Ecommerce users and generic internet users' concerns have not been appropriately addressed in last decade (Foltz & Foltz, 2020).

Data privacy concern is not limited to company customers. Even

healthcare customers have concerns about the collected data in terms of its usage. However, through a survey of many patients, it has been confirmed that privacy does not impact medical hospital selections of patients (Tseng et al., 2020). Pomfret et al. (2020) concluded through research that social media users are willing to pay for their data protection. Schaewitz et al. (2020) studied mobile technologies that offer opportunities for the development of communication in crisis management. The author is of the opinion that smartphones can work towards privacy and build solutions that will give a sense of protection to customers.

Libaque-Sáenz et al. (2020) studied the value of customer collected data and its capitalization when collected through mobile applications. The author concluded that mobile applications must work on ethical concerns of privacy. Users must be given a sense of data protection.

Schurmann et al. (2020) studied user's privacy preferences. Alarmingly, today's users are ready to share more information compared to earlier people without much consideration regarding its privacy. Bordonaba-Juste et al. (2020) studied users' privacy concerns age-wise. The authors concluded that generation X has more concerns compared to generation Y and Z. The reason can be the experience of privacy breach. There is no holistic definition of privacy as it encompasses numerous capacities of human life. Privacy can be informational and physical. However, in the context of online internet usage, privacy is mainly informational.

Online privacy is referred to as privacy paradox. Privacy has economic value. Privacy is a commodity of information system. Privacy has been mentioned as independent good in the world economic forum goods list. Literature exist on cost and benefit analysis of privacy. However, privacy concerns have been addressed in two main categorized in terms of volunteer and volunteer privacy. In some cases, users trust the firms and risk privacy invasion. The customer provision of data is the backbone of many industries. As per the neoclassical economic theory, humans make logical and rational choices based on their preferences. But psychology and behavioral economics says the cognitive biases of the users lead to the sharing of information and trusting of firms. A behavioral aspect also applies to individuals.

Lee (2020) studied the privacy policy of the biggest internet company, Google. The author is of the opinion that least focus has been given on privacy policy and the ability of bigger companies such as Google and Facebook to use consumer data. One of the reasons behind less focus is the scholars' disagreement. The author studied the DoubleClick by Google as a case study for testing the privacy aspects. The author concluded that privacy is an antitrust issue. In-depth analysis of major companies can reveal several aspects of privacy. The solution to privacy issues is the anti-trust movement, which earlier led to privacy laws.

## Discussion

We are living in an information driven economy. Every business can take advantage of data. For business, the free-market view of privacy is more suitable while for the user, consumer protection privacy view is more beneficial. The basic assumption of free-market view is that all users should know the agreement while subscribing or buying the product. The authors conclude that in the case of the web, world's current literacy level does not support the free market view. On websites, most of the companies use cookies; a tracking option which needs in-depth legislation and awareness by users. The companies which collect consumer data get more revenue and set high price tags on consumer's data. The dark side is the consumer's inability to know where their information is being used. In this regard, very few people are aware of what happens to their data.

When researchers asked consumers about further actions on their submitted data, they told that they have no or very little knowledge of it. Many users found data collection very creepy and unfair. Several users realized

first time that they had shared their data with some companies which are using data as source of revenue. Through research, it has been confirmed that not a single organization has the same viewpoint on the understanding of data usage. Every firm uses data as per its own interpretation. Some use data to serve customers better. Some use consumer data for better product development and strategy. While some only measure customer satisfaction. Yet there is no single authority that can define limits of how firms should use data. The core concern of the consumers, is dealing with data once consumers subscribe to a service. Firms have a different viewpoint on how customer email and other information are maintained in terms of record-keeping and profit generation through sales to affiliates. Generally, customers have least access to their information as well as how it is used.

Private information is vital for e-commerce companies. For e-commerce companies, the users share both their personal and financial data. The financial data leakage or any breach of privacy can have multi-fold losses for customers. Should financial information use to buy a product or service is saved or not? If the data is saved, then what should be the level of data protection and how much information should be saved. What kind of framework can be built to secure customer privacy? Some researchers recommended in literature blockchain technology. It is a decentralized technology and can help in handling consumer privacy-related issues. Future researchers are recommended to explore privacy models for big firms such as Amazon and Alibaba. Even though these firms are collecting a vast amount of data, yet these companies have a strong mechanism to protect customer data from theft. Financial information leakage in small firms can have a significant impact. Future models should be based on the consumer protection view.

### Privacy in the Era of Transformative Marketing

There are opposing views regarding which method is more suitable for organizations versus individual consumers. For organizations, free-market view of privacy is more suitable, whereas for individual consumers, the consumer protection view is more suitable. There is a need for in-depth legislation at the country and world level. Consumer awareness also needs to be increased worldwide. Lack of understanding of how consumer data is used by organizations and other stakeholders is dangerous for the consumer, which will hamper business in the long run. Organizations are also needed to be made aware of regarding ethical usage of consumer data.

Organizations are in a better shape to use data due to the presence of technology for the benefit of all stakeholders. The current era as per Kumar & Patel (2014), is of transformative marketing. Organizations can better serve customers by using data. They can make customized products and services, which can create a Win-Win situation for all stakeholders. The market view can be further extended to bring it close to the consumer protection view by informing customers every time their data is used as information by a company. This solution can help the customers to decide whether they should share data with an organization or not.

### Results

Based on the review of literature, it can be stated the vast majority of consumers are unaware of how their personal data is used. Consumers are either too careless in managing their data or too cautious, which may lead to problems for all stakeholders. Basic theories exist for privacy. Their application to online business has been studied to a small extent. There is a need for further study on the online privacy of consumers. Transformative marketing requires consumer involvement at every stage of business. Consumers will only share information if they trust the or-

ganization. Long-term association with consumers is only possible if consumers are well aware of privacy issues and organizational policies to handle consumer data. Organizations must gain and maintain consumer trust by taking care of consumer's privacy concerns. The success of transformative marketing era depends on how consumer privacy issues are handled. It can be said that privacy is truly at the very heart of the success of transformative marketing.

### Conclusion

This article has made a brief review of literature on consumer privacy with a focus on transformative marketing. The current article highlights alarming insight that consumers are unaware and unconcerned how their private data is used for commercial gain without taking their permission. The two views on consumer privacy are shared, and future evolution in these views is discussed. Although the article advocates the consumer protection view; however its evolution is based on free-market view.

The article has also highlighted the government has to play an active role since the issue pertains to the entire world. Areas that need to be focused on by governments, as well as organizations, are highlighted in the article. Lastly, it is emphasized that focus should be on consumers since they are the ones providing actual data, which is very of private nature.

### References

- Aichholzer, G., & Strauß, S. (2010). Electronic identity management in e-government 2.0: Exploring a system innovation exemplified by Austria. *Information Polity*, 15(1), 139-152. doi:<https://doi.org/10.3233/IP-2010-0203>
- Argyriou, E., Kitchen, P. J., & Melewar, T. (2006). The relationship between corporate websites and brand equity: A conceptual framework and research agenda. *International Journal of Market Research*, 48(5), 575-599. doi:<https://doi.org/10.1177/147078530604800507>
- Basu, C. (2009). Disrupting class how disruptive innovation will change the way the world learns. *Journal of Information Privacy and Security*, 5(4), 70-71. doi:<https://doi.org/10.1080/15536548.2009.10855877>
- Bordonaba-Juste, M. V., Lucia-Palacios, L., & Pérez-López, R. (2020). Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services. *Information Systems and e-Business Management*, 1-26. doi:<https://doi.org/10.1007/s10257-020-00462-8>
- Boritz, J. E., No, W. G., & Sundarraj, R. (2008). Internet privacy in e-commerce: Framework, review, and opportunities for future research. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences HICSS*, Hawaii, HI. IEEE.
- Cachin, C. (1997). *Entropy measures and unconditional security in cryptography* (Unpublished doctoral dissertation). ETH Zurich, Switzerland.
- Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1), 3-32.
- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., ... Sheth, A. N. (2014). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Transactions on Computer Systems (TOCS)*, 32(2), 1-29.

- Farooq, M., Kalimuthu, R., & Reza, M. (2019). Measuring and comparing brand equity of Malaysian banks in the era of transformative marketing. *Global Journal of Emerging Sciences, 1*, 96-102.
- Farooq, M., Muhammad, S., Raju, V., Kalimuthu, K. R., & Qadir, A. (2019). Measuring and comparing the desired and actual service quality of Pakistan international airline. *The Journal of Social Sciences Research, 52*, 484-490. doi:<https://doi.org/10.32861/jssr.52.484.490>
- Farooq, M., & Raju, V. (2019). Want to stay the market leader in the era of transformative marketing? keep the customers satisfied! *Global Journal of Flexible Systems Management, 20*(3), 257-266. doi:<https://doi.org/10.1007/s40171-019-00213-w>
- Farooq, M., Rehman, F. K.-U., Tijjani, A. D., Younas, W., Sajjad, S., & Zreen, A. (2019). Service quality analysis of private universities libraries in Malaysia in the era of transformative marketing. *International Journal for Quality Research, 13*(2), 269-284.
- Farooq, M., Zareen, Z., Younas, W., Khalil-Ur-Rehman, K., & Yasmin, N. (2018). Impact of digitalization on Holy Quran readers: Experience and expectations. *IOSR Journal of Humanities and Social Science (IOSR-JHSS), 23*(7), 59-67.
- Foltz, C. B., & Foltz, L. (2020). Mobile users' information privacy concerns instrument and IoT. *Information & Computer Security, 28*(3), 359-371. doi:<https://doi.org/10.1108/ics-07-2019-0090>
- Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*, 719-733.
- Jain, P., & Aggarwal, V. (2015). Service quality models: A review. *BVIMSR's Journal of Management Research, 23*, 125-136.
- Johnson, G. (2017). *Exploring strategy: Text and cases*. London, UK: Pearson Education Limited.
- Klewitz-Hommelsen, S. (2002). Indicators for privacy violation of internet sites. In *Electronic government* (p. 456-459). New York, NY: Springer.
- Knijnenburg, B. P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human-Computer Studies, 71*(12), 1144-1162. doi:<https://doi.org/10.1016/j.ijhcs.2013.06.003>
- Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications, 90*(11), 22-26.
- Lee, J. (2020). The google-doubleclick merger: Lessons from the federal trade commission's limitations on protecting privacy. *Communication Law and Policy, 25*(1), 77-103. doi:<https://doi.org/10.1080/10811680.2020.1690330>
- Libaque-Sáenz, C. F., Wong, S. F., Chang, Y., & Bravo, E. R. (2020). The effect of fair information practices and data collection methods on privacy-related behaviors: A study of mobile apps. *Information & Management, 10*, 32-84. doi:<https://doi.org/10.1016/j.im.2020.103284>
- Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (is) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563. doi:<https://doi.org/10.1057/s41303-017-0066-x>
- Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management, 36*(5-6), 519-549. doi:<https://doi.org/10.1080/0267257x.2020.1715465>
- Ramayah, & Ahmad, H. A. (2010). Service quality dimensions: an examination of Gronroos's service quality model. *European Journal of Marketing, 8*(4), 488-491. doi:<https://doi.org/10.1017/CBO9781107415324.004>
- Roy, I., Setty, S. T., Kilzer, A., Shmatikov, V., & Witchel, E. (2010). Airavat: Security and privacy for mapreduce. In *NSDI: 7th USENIX Symposium on Networked Systems Design and Implementation*, San Jose, CA (Vol. 10).
- Schaewitz, L., Winter, S., & Krämer, N. C. (2020). The influence of privacy control options on the evaluation and user acceptance of mobile applications for volunteers in crisis situations. *Behaviour & Information Technology, 12*, 1-17.
- Schurmann, T., Gerber, N., & Gerber, P. (2020). Benefits of formalized computational modeling for understanding user behavior in online privacy research. *Journal of Intellectual Capital, 21*(3), 431-458. doi:<https://doi.org/10.1108/jic-05-2019-0126>
- Spiekermann, S., & Cranor, L. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67-82. doi:<https://doi.org/10.1109/tse.2008.88>
- Su, S., Fortes, J., Kasad, T., Patil, M., Matsunaga, A., Tsugawa, M., ... Herrera, M. (2005). Transnational information sharing, event notification, rule enforcement and process coordination. *International Journal of Electronic Government Research, 1*(2), 1-26. doi:<https://doi.org/10.4018/jegr.2005040101>
- Tseng, H.-T., Hung, W.-F., Hwang, H.-G., & Chang, I.-C. (2020). Do patients' privacy concerns influence their intention toward medical image exchange consent in Taiwan? *Healthcare, 8*(1), 14-18. doi:<https://doi.org/10.3390/healthcare8010014>
- Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In *Sixth International Conference on Semantics, Knowledge and Grids*, Beijing, China.