

MBAS904: Assessment 1

Part 2- Research Report

Name	Student No.
Chinmay Datar	6956361
Shruti Jawale	6922557

Word Count: 1570

Executive Summary

Ever since the inception of the internet, big data has become an integral part of every industry. One of the biggest industries using big data is e-commerce industry. The competitive advantage gained by using big data to boost revenue, enhance the perceived image of the company and finding your target market is immense.

This report aims to throw light on some of the ethical issues face by the e-commerce industry when storing and using data as well as the concerns raised by the consumers about online shopping. In the modern times e-commerce websites have a big responsibility of safely storing and using the user's data adhering to guidelines established by the governing bodies. Online businesses need to ensure that the privacy and security of the consumers is not compromised in order to gain customer trust and loyalty, thus, creating a sustainable business.

Table of Contents

S. No.	Topic	Page No.
1.	Introduction	4
2.	Ethical Issues in E-Commerce	4
3.	Conclusion	7
4.	References	8

Introduction

Lester states new kinds of threats to privacy are being seen which have their roots in capitalism, free market, advanced technology, and exchange of electronic information (2001, p. 7). Privacy has become a big concern in the modern days since the inception of information technology. In recent times, during the COVID outbreak numerous offline stores shut down and new and existing e-commerce websites have taken their place which at a rapid rate. Additionally, this also paved the path for this business to collect consumer's data and analyse it. When shopping in offline stores the purchased data is aggregated, and the consumer remains anonymous. As we move towards online retail stores this anonymity changes. Individual's shopping trends are collected via transactions and used for targeted marketing, making businesses more efficient and making higher profits. According to experts 61% of users in U.S.A. do not purchase products online due to privacy concerns (Janice, Burke & Nicholas 2004, p. 58). There are growing concerns regarding ethical issues interfering with privacy of consumers and collecting and use of consumer data (Caudill & Murphy 2000, p. 7). This article aims to examine the ethical issues that the online retail stores encounter.

Ethical Issues in E-Commerce

E-commerce has become an inseparable part of our lives in the twenty-first century. With advancement in technology and analytical processes online retailers have better opportunities to offer increasingly tailored advertisements by analysing your personal information (Tucker 2014, p. 546). Personalisation is done using data based on geolocation and buyer persona to meet the consumer's needs and preferences (Yan et al. 2009, p. 261). With highly developed tracking, collaborative filtering and click stream analysis online retail businesses are able to understand individual customers better and translate the insights into offerings and promote their own products and services (Tam & Ho 2005, p. 271). Lewis Strauss' firm adopted personalised advertisements and found their sales to boost as customers were ordering 76% of the recommended products (Cohan 2000, p. 9).

However, many consumers raised concerns regarding the ethics and security of the data online. Miyazaki and Fernandez (2001, p. 27) evaluated these concerns and categorised them into 3 categories of ethical issues: (1) Privacy, such as sharing of personal information, spam contacts from online retailers and tracking of online shopping behaviour; (2) Security, including concerns regarding malicious individuals who could potentially breach data security and attain personal, financial, or transactional information; (3) fraud, focusing on concerns regarding dishonest behaviour by the online retailer, including intentional misrepresentation or non-delivery of goods. Fraud also includes online scams such as fake e-commerce websites or fake sellers on online retail websites. These concerns exist because the e-commerce business grew faster than ethical standards could be established and implemented. By categorising the concerns of the consumers, we can have a clear idea of the issues that need to be tackled by the government and the online retailers alike, to reassure the consumers of a safe online shopping experience.

Privacy and security have become the two major concerns in the online retail industry since the inception of e-commerce (Roman & Cuestas 2008, p. 641). In most cases, consumers are unaware that their online presence is being tracked by the ecommerce organizations as soon as they visit the website. This is done by creating a small file on your system i.e., cookies. This file stores data on your device to track your activities on the website, identify repeat visitors and help the store personalize the shopping experience.

One popular example of invasion of privacy is an infamous educational toys website named Toysmart. The website collected detailed information about their visitors including name, address, billing information, shopping preferences, and family profiles. In September 1999, Toysmart posted a privacy policy which stated that information collected from customers will never be shared with third parties. When the company ran into financial crisis, it attempted to sell all of its assets, including its detailed customer databases when their privacy policy stated otherwise. After a lawsuit the sale of the customer was prevented and the company went bankrupt (Roman & Cuestas 2008, p. 641).

Miller and Weckert (2000, p. 52) argue that being an online retailer does not give right to gather information and distribute to other vendors at a profit. Information collected by cookies and ill intended services are not necessary for any business transaction. The self-serving motive of increased profitability is in conflict with user's right to privacy especially

considering that some customers would not want to be served this way (Stead & Gilbert 2001, p.75).

Security is one of the critical factors in determining the success or failure of an online retailer (Prasad & Aryasri 2009, p. 73). While conducting online transactions customers are worried that the store will cheat them or use their personal information, like their credit card details (Comegys et al. 2009, p. 295). People in brick-and-mortar settings, like a restaurant, will commonly risk giving their credit card to an unknown waiter for billing, but they will avoid doing the same in case of an online retailer.

Here the problem isn't necessarily with the online retailer, but the security breaches that can arise as the credit card info travels down the communication line to reach the e-commerce computer (Kracher & Corritore 2004, p. 81). It is understandable that the customers will hesitate in sharing their personal information due to the untrustable nature of the security of online transactions. Although an online retailer might adhere to the standard security measures based on technological solutions and legal guidelines, it won't necessarily be enough as the customer's perceived sense of security is required to build trust in the online transaction process (Pavlou & Chellappa 2001, p. 358).

Another major concern related to online shopping is fraud. As mentioned above, fraudulent behaviour by online retailers encompasses various issues, one of the main ones being the financial risks associated with it. The definition of financial risk is the potential loss of money as well as the customer's sense of security with respect to using credit cards for online transactions (Elbeltagi & Agag 2016, p. 288).

With online shopping there's a risk of receiving an unwanted or low-quality products, sometimes the ordered product may not even match the given description (Comegys et al. 2009, p. 295). In some cases, fraudulent retailers may not even deliver the products, but the customer is notified of a successful delivery and the money is debited. In spite of these issues, the retailers may not agree to refund the customer for those products (Katawetawaraks & Wang 2011, p. 66). This type of fraudulent behaviour reduces the degree of trust the customer places in e-commerce businesses.

Solution to all these concerns is having appropriate guidelines and laws in place for online retailers to adhere to. By doing this, retailers can enhance the customers perceived sense of

security thereby improving their own sales and the shopping experience for the customer. Some of the ways this can be achieved are (Turban et al. 2012, p. 736):

Notify the consumers: The online retailers should notify the customers beforehand regarding their data collection practices. On the basis of this information customers can make an informed decision about the type and extent of the disclosures.

Consumer consent: Consumers must be made aware of the options available to them as to how their personal information may be used for any type of intents and purposes. By offering opt-out clause consumers have the choice to consent the use of their information.

Data integrity: The online retailers should take necessary measures to assure the consumers that their personal data is secure and accurate. This includes holding the retailers responsible for the loss of data, unauthorized access or alteration, destruction, and fraudulent use. They need to ensure that the information is gained from reputable and reliable sources.

Enforcement: There should be an entity like the government, to enforce the privacy clauses, otherwise there is no reliability on these clauses.

Conclusion

The rapid growth of the e-commerce industry has brought along a host of ethical issues. This has made consumers wary of online shopping in spite of the convenience it offers. The looming threat of misuse of their personal information has increased the privacy and security concerns among shoppers. Online sellers need to identify the solutions that can eliminate these concerns and offer the consumers a safe shopping experience.

Like any community, e-commerce also requires a framework built on pre-existing values (Kracher & Corritore 2004, p. 81). To persuade consumers to shop online, retailers should first focus on finding ways to reduce the negative factors and work on gaining their trust. Trust is the key to a successful e-commerce business and ensuring its continued success (Marcella 1999).

Due to the ubiquitous nature of the internet, one can find that the issues presented in this report are quite common in the e-commerce sector. Due to the spotlight on these issues, retailers ensure that they are resolved to avoid perceived exposure and reaction from the public or market (Stead & Gilbert 2001, p.75).

However due to the constant surge of new retailers in the online market trying out inventive tactics, new ethical issues are bound to rise eventually. Timely policing and self-regulatory measure can be implied to ensure that an ethical e-commerce environment can be maintained. The failure to adhere to the ethical guidelines that ensure a safer shopping experience for consumers can result in severe repercussions including heavy financial losses and a tarnished brand image.

References

- Lester, T 2001, 'The Reinvention of Privacy', *The Atlantic Monthly*, vol. 287, no. 3, pp. 27–39.
- Caudill, EM & Murphy, PE 2000, 'Consumer Online Privacy: Legal and Ethical Issues', *Journal of public policy & marketing*, vol. 19, no. 1, pp. 7–19.
- Sipior, JC, Ward, BT, & Rongione, NM 2004, 'Ethics of Collecting and Using Consumer Internet Data', *Information Systems Management*, vol. 21, no. 1, pp. 58-66.
- Tucker, C. 2014, 'Social Networks, Personalized Advertising, and Privacy Controls', *Journal of Marketing Research*, vol. 51, no. 5, pp. 546–562.
- Tam, KY & Ho, SY 2005, 'Web Personalization as a Persuasion Strategy: An Elaboration Likelihood Model Perspective', *Information Systems Research*, vol. 16, no. 3, pp. 271-291.
- Cohan, P. S. 2000, 'E-Profit: High-Payoff Strategies for Capturing', *The E-Commerce Edge*. AMACOM, New York.
- Miyazaki, AD & Fernandez, A 2001, 'Consumer Perceptions of Privacy and Security Risk for Online Shopping', *Journal of Consumer Affairs*, vol. 35, no. 1, pp. 27-44.
- Yan, J, Liu, N, Wang, G, Zhang, W, Jiang, Y, Chen, Z 2009, 'How much can Behavioral targeting help online advertising?', *International Conference on World Wide Web—WWW '09*, pp. 261-270.

- Román, S & Cuestas, PJ 2008, 'The Perceptions of Consumers regarding Online Retailers' Ethics and Their Relationship with Consumers' General Internet Expertise and Word of Mouth: A Preliminary Analysis', *Journal of business ethics*, vol. 83, no. 4, pp. 641–656.
- Miller, S & Weckert, J 2000, 'Privacy, the Workplace, and the Internet', *Journal of Business Ethics*, vol. 28, no. 25, pp. 52-63.
- Stead, BA & Gilbert, J 2001, 'Ethical Issues in Electronic Commerce', *Journal of business ethics*, vol. 34, no. 2, pp. 75–85.
- Prasad, C & Aryasri, A 2009, "Determinants of shopper behaviour in e-tailing: An empirical analysis", *Paradigm*, vol. 13, no. 1, pp. 73-83.
- Comegys, C, Hannula, M, & Váisänen, J 2009, 'Effects of consumer trust and risk on online purchase decision-making: A comparison of Finnish and United States students', *International Journal of Management*, vol. 26, no. 2, pp. 295-308.
- Kracher, B & Corritore, CL 2004, 'Is There a Special E-Commerce Ethics?', *Business ethics quarterly*, vol. 14, no. 1, pp. 123–67.
- Chellappa, R & Pavlou, P 2002, 'Perceived information security, financial liability and consumer trust in electronic commerce transactions', *Logistics Information Management*, vol. 15, no. 5, pp. 358-368.
- Elbeltagi, I & Agag, G 2016, 'E-retailing ethics and its impact on customer satisfaction and repurchase intention', *Internet Research*, vol. 26, no. 1, pp. 288-310.
- Katawetawaraks, C & Wang, CL 2011, 'Online Shopper Behaviour: Influences of Online Shopping Decision', *Asian Journal of Business Research*, vol. 1, no. 2, pp. 66-74.
- Turban, E, King, D, Lee, J, Liang, TP & Turban, D 2012, *Electronic commerce 2012: a managerial and social perspective*, 7th edn, Pearson Education, New York.
- Marcella, AJ 1999, 'Establishing Trust in Virtual. Markets.' *Altamonte Springs, FL*, The Institute of Internal Auditors.