International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:08, Issue:05 "May 2023"

DATA PRIVACY ISSUES WITH E-COMMERCE

Dhruv Arora

Salwan Public School, Gurugram

DOI: 10.46609/IJSSER.2023.v08i05.020 URL: https://doi.org/10.46609/IJSSER.2023.v08i05.020

Received: 25 May 2023 / Accepted: 31 May 2023 / Published: 5 June 2023

ABSTRACT

This paper focuses on the data privacy issues that arise with the utilization of e-commerce platforms, focusing on the challenges and ability to protect a consumer's data in an online transaction. As the popularity of e-commerce continues to grow and new platforms tend to rise, security and privacy concerns of personal information become supreme. This paper explores aspects of data privacy and multiple criteria of concerns that come along with it. It also discusses note-able privacy breaching incidents in this industry and how one can be safe within such digital bubble. Additionally, this paper talks briefly about the government regulations and legal framework that keeps a check over them along with a common consumer's point of view towards it.

Introduction

With the recent developments around the world especially the growth in the tech sector, there has been a major increase in the number of users switching to an online based marketing environment. With its ever-growing significance, users have named it E-Commerce (Electronic Commerce).

E-Commerce is term given to buying and selling of goods and services over internet. It draws on technology such as mobile commerce, electronic fund transfer, supply chain management, data collection systems, etc. It forms up the largest sector of the electronic industry.

The internet usage in the sector of commerce has been flourishing ever since its invention and the offline retailers and whole sellers are shifting online to the e-commerce platforms on an ever-growing rate. Even though there have been promising results, it raises a major concern for security as puts us and our safety vulnerable to the outside party. The growing rate of literacy and the day-to-day usage of our devices has led to a state where we tend to trust our commerce agents and the service providers too much to be able to second thought the data which we provide in return. The main concern is the works of the platform and how well can they work of confidentiality of the data which their users provide. This research paper talks about the privacy issues and how the public can prevent them from happening.

Why is it concerning

Data privacy has become a major issue in this age. Everything and everyone are available digitally and so are the trade and shopping websites. However, such presence holds a possible threat. These are a few points explaining them-

- **Collection of Personal Data:** Collection of data in the e-commerce websites is more or less, a necessary evil. Collection of data allows a more user friendly and personalized environment for a consumer along with letting them browse and access the portal seamlessly. Although, comes with a risk factor being the availability of it throughout the servers, leaving it vulnerable for misusers.

- **Sharing of Personal Data:** Certain e-commerce websites tend to allow third parties such as sellers or advertisers to provide content which would synchronize with the previously done searches. This allows them to access a new marketplace and a more user interaction-based platform is created.

- **Lack of Transparency:** E-commerce platforms are not always transparent about their usage of data. Customers may not be aware what goes on with their data, how it is stored and managed. This tends to build a possible un-friendly relationship between the platform and the customer.

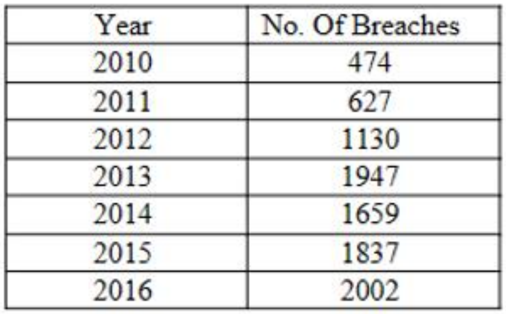
- **Cybersecurity Threats:** E-commerce platforms as we know, are vulnerable to cyber threats. Having an un-secure and a careless management can lead to a possible theft of intellectual property or misuse of stolen data.

- **Data Protection Laws-** E-commerce platforms are supposed to follow the legal regulations provided to them. Failure to comply with them can result in possible legal actions and public backlash. General Data Protection Regulation (GDPR) in the EU and the Personal Data Protection Bill in India are two such set of amendments they must follow. However, most companies tend to ignore since following the geographically based server management of data requires a much larger capital investment.

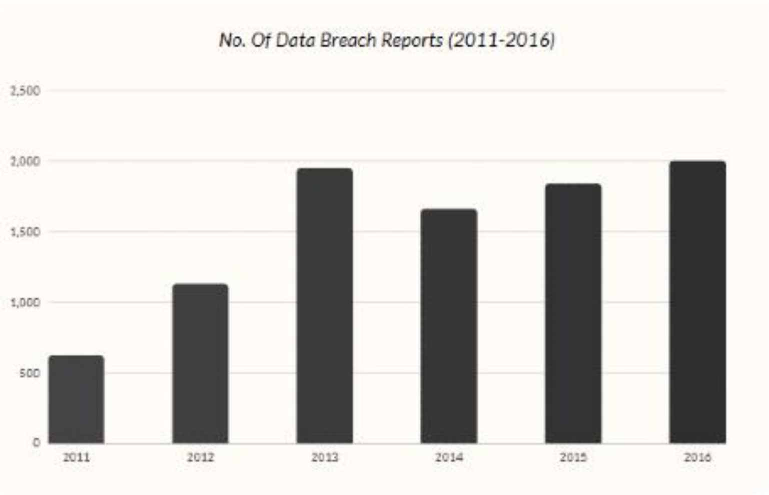
- **Use of Cookies and Tracking Technologies:** Cookies are a particular set of instructions and commands provided to the end user to give allowance to their data being shared. “This website uses cookies” pop up which we may tend to ignore, carry a major possible risk factor along with them. E-commerce platforms may use cookies and other tracking methods. The collected data is further used to provide targeted adverts and marketing but it can also infringe on a consumer's privacy.

- **Customer Trust:** Data privacy issues can erode customer trust in e-commerce platforms. Customers are more likely to do business with companies that they trust to protect their personal information.

Following chart shows the number of data breach reports received in US-



Year	No. Of Breaches
2010	474
2011	627
2012	1130
2013	1947
2014	1659
2015	1837
2016	2002



Source- Data breach reports | Mass.gov

Why dealing with it is necessary-

- **Identity Theft:** E-commerce platforms collect a significant amount of data from their consumers such as their names, numbers, search history and other relevant data required for a better user interface. This data can be used by cybercriminals and can have consequences.

- **Fraudulent Activities:** Data Breaches on e-commerce platforms may lead to fraudulent activities such as fake transactions and unauthorized purchases.

- **Breach of Trust:** E-commerce platforms are expected to maintain a certain standard regarding their data privacy and safety practices. If a data breach occurs, would lead to a fall in trust and goodwill of that platform.

- **Legal Consequences:** As mentioned above, GDPR and Personal Data Protection Bill safeguards the ability of a platform to continue using un-safe processes. If they fail to follow and rule out the vulnerabilities, they will be fined and may undergo a legal procedure.

- **Competitive Advantage:** Data privacy issues may lead to a loss of competitive advantage due to companies preferring doing business with a platform they would be able to trust and have a good relation with.

- **Reputation and PR Damages:** E-commerce platforms that suffer with data damages may also deal with a damaged public image and a reputation that would carry a possibility of further moving away customers.

Data privacy issues arising in e-commerce is an issue for both, the platform as well as its users. It is our social responsibility to use it in a manner which would minimize potential damage for both the parties.

To further explain, let us take some more historical facts to explain the importance.

Timeline of popular privacy breaches and issues-

1. **Sony PlayStation Network Breach-** April 2011, Sony discovers an unauthorized access in the PSN network and services. By the time, the breach had compromised 77 million PSN user accounts. This breach was further spread to Sony Online Entertainment (SOE) affecting an extra 24.6 million accounts. Stolen data contained information such as addresses, names and personal information including credit and debit card data. The breach had a signification financial fallout for Sony costing them around $171 million including all kinds of legal and short-term expenses. Furthermore, Sony had to close the PlayStation Network for almost a month. The breach also attracted legal attention and left Sony with lawsuits from multiple parties. This incident thrashed Sony's reputation and goodwill of a reliable service provider.

2. **eBay Data Breach-** In the early May 2014, eBay discovered an unauthorized access to their corporate and consumer database. The breach had resulted in a compromise of 145 million eBay users across the world. Unlike some other high-profile breaches, eBay's breach did not carry a threat to user's financial data. eBay stated that they store the user base's financial information secured separately.

3. **Twitter Data Breach- The** 2020 Twitter data breach is a cybersecurity incident that occurred on July 15, 2020 where the attackers managed to gain control of accounts

belonging to prominent individuals to promote a cryptocurrency fraud. The effected accounts were made to tweet out a link asking for a certain amount of money to a crypto wallet, promising a better return. Twitter took immediate action to restrict such unauthorized tweets.

Some major e-commerce related financial data breaches-

Year	Organization	No. Of Records Breached	Remark
2007	TJ Maxx	94,000,000	Earlier, known large data breach. Hackers stayed within the network for 18 months un-detected.
2013	Target	70,000,000	Unauthorized access from sales system.
2014	Home Depot	56,000,000	Attack originated at self-service POS terminal.
2013, 2014	Yahoo	1,000,000	Two breaches discovered around 2016 having long lasting security consequences.
2018	Marriott	500,000,000	Unauthorized access through Starwood guest database, a Marriott International's subsidiary. Went on for 4 years un-noticed.

How to prevent data privacy attacks

- **Strong Security Measures:** E-commerce platforms should maintain a database according to the legal requirements. A regular check is also necessary to maintain security standards.

- **Transparency-** E-commerce platforms should be transparent regarding their database management and security technologies.

- **Limit Data Collection-** E-commerce platforms should limit collection of unnecessary data and should work upon getting rid of it periodically to prevent leaving the extra information vulnerable.

- **Training Employees-** Employees should be trained to manage and minimize possible issues regarding the data and work upon making the network safer.

- **Fulfilling Legal Requirements-** E-commerce platforms are supposed to comply with the laws such as GDPR and the Personal Data Collection Bill in India.

- **Use Trusted Third-Party Vendors:** Third party vendors for payment and shipping allow the extra work to be outsourced and leave less room for data breaches. Moreover, government-based vendors would also be a great way to minimize the work.

- **Provide Customer Support:** E-commerce platforms should provide a better and a more responsive customer support to their users. In case of a data breach, customer report can surely help in locating it.

A consumer's point of view

From a consumer's point of view, data privacy issues can give rise to a range of attitudes and concerns.

- **Privacy Protection-** Consumers tend to value their information and expect the platform to prioritize it. An assurance is required that their data shall remain secured and no threat to an intellectual property should occur.

- **Transiency and Trust-** A consumer expects and appreciates total transparency from a business or a platform. The privacy policies listed should be clear and easy to understand. Trust is an important aspect of trade. Since it involves financial concerns, trust is necessary to be matched.

- **Control over Data-** Consumers do enjoy extra control over their personal data. Ability for them to manage it themselves and being able to customize it adds an extra layer of trust. They appreciate the options such as being able to customize their email preferences or what data is displayed and what is being shared to the third parties.

- **Awareness and education-** Consumers and sellers are required to be digitally literate and should be provided education about being safe while browsing. Costumers value clear education and communication on data privacy. Being educated empowers them to further interact with the platform and feel safe while doing so.

- **Personalization of experience-** Even though privacy is import, a visually appealing personalized experience seems too much to lose. Consumers may be willing to share data and lose privacy to receive tailored experience, improved shopping recommendations and offers. However, a way where you get to enjoy these as well as receive data privacy would surely give the consumers an extra layer of trust.

A consumer just requires user-friendly environment with no risk factor involved. A consumer is asking for it since a monetary exchange involved, providing them with the right to use of that certain good or service. It is a necessity that the platform and the business to maintain that level of trust. Consumers are increasingly being made aware of the importance of being safe in this digital world, they expect the platforms to prioritize their safety. Customers are increasingly starting to evaluate a company's trustworthiness along with their reputation on the privacy practices they follow.

Conclusion

In conclusion, data privacy concerns in recent years have emerged as a critical area of significance, drawing attention from everyone whether it is a common user or a researcher. The rapid high paced advancement of technology recently has boosted the collection and utilization of personal information by online businesses. It is crucial for these platforms to address these concerns regarding privacy and ensure public understanding. The growing need and demand for matters concerning data privacy rights makes us aware about the need for progressive research, efforts and the establishment of regulations which would act effectively to insure a trustworthy, privacy-based environment for users.

References

Srinivasan, S. (2015). Privacy protection and data breaches. Proceedings of informing Science & IT Education Conference (InSITE) 2015, 429-444.

http://proceedings.informingscience.org/InSITE2015/InSITE15p429-444Srini1984.pdf

Mark. S. Ackerman, Lorrie Faith Cranor, Joseph Reagle. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences

https://dl.acm.org/doi/pdf/10.1145/336992.336995

Aivazpour, Z., Valecha, R., Chakraborty, R. (Forthcoming). Data Breaches: An Empirical Study of the Effect of Monitoring Services. The Data Base for Advances in Information Systems, In Press.

https://www.researchgate.net/profile/Zahra-Aivazpour/publication/334726367_The_Impact_of_Data_Breach_Severity_on_Post-

Breach_Online_Shopping_Intention/links/61969b1307be5f31b796d58d/The-Impact-of-Data-Breach-Severity-on-Post-Breach-Online-Shopping-Intention.pdf

Muneer A, Razzaq S, Farooq Z (2018) Data Privacy Issues and Possible Solutions in E-commerce. J Account Mark 7: 294. Doi: 10.4172/2168- 9601.1000294

https://pdfs.semanticscholar.org/27aa/a579dc1f178d8e636616cc3b57658c44a3b7.pdf