Protection of Online Privacy of Consumers in E-Commerce

T. H. Desai
Department of Law, Veer Narmad South Gujarat University, Surat, India

Keywords: Online Privacy, E-Commerce, Consumer Protection.

Abstract: The rapid growth of e-commerce has led to increased concern about the protection of online privacy for consumers. Online privacy refers to the protection of personal information collected, stored, and processed by e-commerce companies. In recent years, there have been several high-profile data breaches that have raised concerns about the security of personal information online. It is important to implement strong data protection laws and security measures, increase transparency, and give individuals greater control over their personal information. The present paper deals with various issues and concerns regarding online privacy violation arising in E-commerce focusing on various modes through which it is perpetrated and further analyses the existing legislative framework in curbing such instances while giving some useful suggestions for prevention of online privacy violation in E-Commerce transactions.

1 INTRODUCTION

Computers, internet and information technology has invaded every aspects of human life. Information technology has also taken over the world of business introducing us to the concept of E-commerce. The rapidly growing E-commerce industry has removed geographical restrictions and connected various businesses and consumers with each other via the medium of information technology. Internet has enabled people to do more and more things in the virtual world. Along with the expanding scope of internet, the very face of business has also changed. The business and commerce has resorted to internet in order to maximise their profits thereby shifting their addresses from physical brick and mortar shops to the virtual world of internet thereby emerging in the form of E-Business and E-Commerce. With Government allowed FDI in multi-brand retail shops on e-commerce platform, a wide range of products became available to consumers making the whole shopping experience easy and convenient. Along with countless advantages of E-commerce, there are those taking unfair advantages and misusing the internet for their own selfish and reprehensible purposes of which the consumers are mostly unaware of. Many legal issues have also arisen due to large scale expansion of E-Commerce. Hence, in this new era of E-Commerce, the protection of consumer rights has become of utmost importance. One such issue is that of violation of online privacy in E-Commerce. The lack of consumer discretion in dissemination of personal information during online transactions has led to increased risk of violation of online privacy.

2 PRIVACY

The term "Privacy" may be described as "the right to be left alone", or the right to have control over one's personal information, or a set of conditions necessary to protect dignity and autonomy of an individual.

The 'Right to Privacy' has been originated in 1890. (Warren, et al., 1980). The right to privacy is the right to be free from secret scrutiny and to determine whether, when, how, and to whom, one's personal or organisational information is to be revealed.

The right to privacy has also been guaranteed under various international instruments like Universal Declaration of Huma Rights, International Covenant on Civil & Political Rights, 1966 and European Convention on Human Rights, 1950. Right to privacy is not directly protected as a fundamental right under Indian Constitution. However, the Apex Court in case of R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 642 held that right to privacy is included within the ambit of right to life and liberty under Article 21 of the Indian Constitution.

Desai, T.
Protection of Online Privacy of Consumers in E-Commerce.
DOI: 10.5220/0012515600003792

In *Proceedings of the 1st Pamir Transboundary Conference for Sustainable Societies (PAMIR 2023)*, pages 860-863
ISBN: 978-989-758-687-3

Moreover, in Justice K.S. Puttaswamy v. Union of India AIR 2017 SC 4161 : (2017) 10 SCC 1, the Supreme Court, in a petition that questioned the constitutional legality of the Aadhar-based biometric system, unanimously held that the right to privacy is a fundamental right protected by the Constitution. The Court widened the scope of Article 21 and declared that the right to privacy is included in the purview of right to life and liberty.

3 CONSUMER PRIVACY IN E-COMMERCE

Right to privacy in E-commerce means protection of personal information and personal data of a person in E-commerce. The exchange of personal information and data is inevitable for a successful transaction in E-commerce thereby resulting in the consumer information ending up in the hands of people who take advantage of this sensitive personal information for their own selfish intentions which results in violation of privacy in E-commerce.

Consumer privacy is concerned with how the manufacturer or service provider uses and collects the information the consumer provides to him. There is a betrayal of consumer trust in the seller when there is a misuse of information provided by him. There are various modes in which this information may be misused.

Increasingly, data that is collected from consumers is stored in databanks which is then used for both legitimate purposes (such as marketing, research etc.) and illegitimate extraneous purposes (as when this data is sold in bulk to third parties).

4 REASONS FOR VIOLATION OF PRIVACY IN E-COMMERCE

Lack of Awareness: There has been a growing trend among customers to sacrifice convenience for the demand for privacy. Thus, the consumers puts a large amount of trust on the organisations and they do not think twice about sharing their personal information with them without any regards to basic precautions that should be taken by any consumer.

Jurisdiction: In most of the cases, privacy breach in E-Commerce is a trans-border occurrence. Thus, the victim of the breach i.e. the consumer is in one country while the person responsible for the breach may well be thousands of miles away in other country. This creates a huge problem of jurisdiction when the time comes to bring action against the perpetrator.

Lack of uniformity in legislation in various countries: International norms are created for the data protection by UNCITRAL (UNCITRAL Model Law on Electronic Commerce, 1996), OECD (OECD, et, al, 2016), European Union (REGULATION (EU) 2016/679 General Data Protection Regulation) and other international organisations. However, these international norms are either adopted partially or are not adopted at all.

Occurrence of cybercrimes: Invasion of privacy of the consumers is a huge concern as it violates the basic fundamental rights of the consumers. However, a bigger concern is the occurrence of cybercrimes like identity theft, internet fraud, bank fraud, cyberstalking, extortion etc. One common factor in all these crimes is the stealing of sensitive personal information of the consumers and using it for furtherance of the offences.

5 LEGISLATIVE FRAMEWORK

India's sole legislation dealing law relating to Information Technology is Information Technology Act, 2000 which deals with cybercrimes and electronic commerce. The Act was enacted keeping in mind the provisions of United Nations Model Law on Electronic Commerce, 1996 (UNCITRAL Model).

Information Technology Act, 2000: The primary law in India that controls how information technology is used and establishes a framework for the protection of personal data is the Information Technology (IT) Act, 2000. The legislation and its regulations are intended to control how digital information is used, encourage the development of the digital economy, and guarantee the preservation of people's rights to their personal data.

Explanation (iii), Section 43A of IT Act, 2000 defines "sensitive personal data" as data related to an individual's financial, health, sexual orientation, biometric, or religious information. The Act requires organizations to obtain written consent from individuals before collecting, processing, or storing sensitive personal data.

The Act requires organizations to implement reasonable security practices and procedures to protect personal data from unauthorized access, alteration, destruction, or disclosure. Furthermore, the Act also requires organizations to notify individuals in the event of a data breach that results in

the unauthorized access, alteration, destruction, or disclosure of their personal data.
The Act imposes criminal liability on individuals who gain unauthorized access to personal data or sensitive personal data stored in a computer resource and provides for various offences related to data protection, including unauthorized access to computer systems, theft of computer resources, and the disclosure of sensitive personal data. Penalties for these offences include fines and imprisonment as laid down under Section 43A and 72A of IT Act, 2000.
However, further rules were required for the implementing these provisions. Thus, as per the requirements of the society, the Government framed the necessary rules to the IT, Act, 2000 which are as follows:

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009
The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

To ensure more uniform consumer and personal data protection across EU member states, GDPR standards are applicable to all EU members. The GDPR's main privacy and data protection regulations include the following:

Requesting people' permission before processing their data Using anonymization to safeguard acquired data's privacy Notifying users of data breaches Managing the cross-border flow of data in a secure manner Mandating the appointment of a data protection officer to manage GDPR compliance for certain firms

6 CONCLUSIONS

Looking at the advanced level of legislations formulated by the developed nations, one can conclude that India is still struggling to come up with an effective and concrete legislation for data protection of the consumers. A legislation dedicated solely with the protection of data and information present on the web is the dire need of the day. Every day without a law protecting the consumer’s privacy is risking exposure to their data and thereby threatening their right to privacy in the digital era. The laws enacted in future must be of international norms which will increase consumer trust and which, in turn, will lead to expansion and development of E-Commerce in India.

There are several key measures that can be taken to improve data protection laws and ensure greater privacy for individuals:

Strengthening data security measures: Governments should require companies to implement stronger data security measures, such as encryption and multi-factor authentication, to protect sensitive information from cyberattacks.

Increased Transparency: Companies should be required to be transparent about their data collection, use, and sharing practices. This would give individuals greater control over their personal information.

Right to Access: Individuals should have the right to access their personal information held by companies and to correct any inaccuracies.

Right to be Forgotten: Individuals should have the right to request that their personal information be deleted by companies.

Data Portability: Individuals should be able to easily transfer their personal information from one company to another, in order to encourage competition and give individuals greater control over their data.

Data Minimization: Companies should be required to collect only the minimum amount of personal information necessary to provide their services, and to retain this information only for as long as it is necessary.

Data Protection by Design: Governments should require companies to build data protection into their products and services from the outset, rather than as an afterthought.

Independent Oversight: Governments should establish independent data protection agencies with the power to enforce data protection laws and investigate violations.

International Cooperation: Governments should work together to harmonize data protection laws across borders, in order to provide a consistent level of

protection for individuals regardless of where their data is processed.

Implementing these measures would help to create a more robust and effective framework for data protection, and would give individuals greater control over their personal information and greater confidence in the security of their data..

REFERENCES

Warren and Brandies (1980). The Right to Privacy, Harvard Law Review, IV (5)
UNCITRAL Model Law on Electronic Commerce, 1996
OECD (2016), OECD Recommendation of the Council on Consumer Protection in E-Commerce, OECD Publishing, Paris
REGULATION (EU) 2016/679 General Data Protection Regulation, 2016
Information Technology Act, 2000 (India)
Consumer Protection Act, 2019
Digital Personal Data Protection Act, 2023
The California Consumer Privacy Act, 2018 (United States of America)
The Personal Information Protection and Electronic Documents Act, 2000 (Canada).