

INDIAN JOURNAL OF LEGAL REVIEW



VOLUME 3 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION



Indian Journal of Legal Review [ISSN - 2583-2344]

(Free and Open Access Journal)

Journal's Home Page – <https://ijlr.iledu.in/>

Journal's Editorial Page – <https://ijlr.iledu.in/editorial-board/>

Volume 3 and Issue 1 of 2022 (Access Full Issue on – <https://ijlr.iledu.in/volume-3-and-issue-1-of-2023/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijlr.iledu.in/terms-and-condition/>

Privacy protection in e-commerce from self-regulation perspective

Authors: Rishav Sengupta, Student of CHRIST (Deemed to be University), Bangalore

Best Citation - Rishav Sengupta, Privacy protection in e-commerce from self-regulation perspective, Indian Journal of Legal Review (IJLR), 3 (1) of 2023, Pg. 370-376, ISSN - 2583-2344.

Abstract

Internet was created in the year 1983 and since then internet serves as a platform for commercial transactions. To speed up commercialization, online commercial methods were developed. Over time, the internet expanded enormously, which boosted commercialization online. E-commerce is another name for online commerce. E-commerce has altered the conventional approach and brought all businesses and customers together under one roof where they can easily interact with one another. Privacy is a key component of e-commerce, and protecting the community's right to privacy is critical. E-commerce increases the danger for consumers involved in e-commerce transactions while offering them little power to defend their right to privacy. Self-regulation is considered as a practical solution for maintaining consumer security and legal protection in e-commerce transactions. The United States places emphasis on a self-regulation model. India has not yet fully grasped the self-regulatory issue of preserving data privacy in e-commerce transactions. Business participants and consumers must act quickly to self-regulate in order to guarantee that consumers' privacy rights are protected in e-commerce transactions.

Introduction

Commerce is the exchange of goods, services, and other things of value between businesses and organisations or individuals; it's an age-old concept. With the advent of computer system, especially the internet, commerce has shifted to virtual platform. Trading in virtual mode falls under the category of electronic commerce or e-commerce. Organisations prefer e-commerce because of its ease of use and efficiency. The vast development in network technology has made electronic transactions among companies with other firms and individual consumers a good and viable option. Hence, buying / selling of products or services through platforms over the internet / world wide web / email has become common in modern times. Such a widespread system brings along security and privacy issues with it. Privacy protection has become a very important issue. Today's e-commerce transactions typically necessitate disclosure of a good volume of personal data like credit card information, delivery details and personal identification details on the virtual platform. Businesses acquire these details for the furtherance of trade. The possession of such information allows businesses to analyse it, discover trends and enhance the efficiency of their business dealings.

The worldwide web has changed the way of doing business and consumer transactions. People can access websites that are launched in a foreign country. As a result of which people can buy or sell goods and services, domestically and across borders. This brings in the concept of international monetary transactions for which domestic consumers and businesses have to upload critical information. Pre-requisite of e-commerce is availability of relevant and accurate information of consumers which is now accessible to any person sitting anywhere in the world.⁹⁶⁴Such international transactions take place based on business-to-consumer trust. What if online shops vanish after online

⁹⁶⁴ Abdul Halim Barkatullah, Djumadi, Does self-regulation provide legal protection and security to e-commerce consumers? Electronic Commerce Research and Applications, 30, 94 - 101, (2018)

payment? Or the seller or any third-party misuses information to steal consumers' identity without their permission?

A seller's identity and genuineness compared to that of a buyer can be easily hidden on virtual platform. Less secure payment system and lack of privacy in data protection can lead to a lot of fraudulent market practices. Such malpractices will begin to question the concept of trust and can easily result in consumer's loss of trust in the buyer and subsequently the virtual platform on which revolves the very existence of e-commerce. In such cases, protection from state laws can be of little or no help due to jurisdictional problems across borders.

Previously, consumers were unaware of the potential uses for which the internet sellers could put their personal information to use, and they were also unaware of any potential privacy violations. But during the past ten years, consumer awareness of privacy has increased, especially among internet users. As a result of their growing demands for e-commerce to respect their privacy, legislation to do so is now necessary. It raises the issue of self-regulation in regards to safeguarding personal data.

Issue

Privacy protection of consumers on online trading platform is a major concern. The concept of self-regulation is one of the ways of protection of privacy apart from state legislations. We shall address the issue of privacy protection by means of implementation of self-regulation policies. In the process, we will refer to United States self-regulation policies implemented to protect consumers' private information and India's take on self-regulating e-commerce platforms.

Analysis

Trust is essential for the expansion of electronic trade between parties that have never done business together. Governments, international organisations, platforms for international electronic commerce, national organisations, and consumer advocacy groups like the European Union, the Global Business Dialogue

on Electronic Business, and the Organization for Economic Cooperation and Development (OECD) have all acknowledged self-regulation as a powerful tool for fostering trust in electronic commerce. So, the process by which businesses that conduct business online voluntarily decide to follow a set of behavioural rules is known as self-regulation. Self-regulation can take several forms, such as establishing a code of conduct or enrolling in a national or international trustmark programme. A trustmark signifies that a website has passed specific digital security checks or is run by an organisation with a specified level of professionalism. States can significantly contribute to the development of self-regulation tools by fostering their development, adopting their own codes of conduct for electronic commerce, and pledging to adhere to specific norms of behaviour for business electronic communications. International electronic commerce would benefit if self-regulation tools like trustmark programmes and codes of conduct adhere to some fundamental standards and uniformity. Global internet commerce would also benefit from the accreditation of self-regulation tools on a global scale.

Implementing self-regulation by online sellers to protect consumers' private data requires rigorous data protection business models and a government data protection policy.⁹⁶⁵ Some countries have standardised how sellers store, use, display private customer information by combining privacy principles with the code of practice regarding transactions through websites. Procedures guaranteeing the security of transactions, such as the use of cryptography or digital signatures, should be followed to guarantee the protection of consumers' data. In online transactions, consumers' private information can be legally protected in accordance with the state's statutory requirements and with the restrictions established by the seller, such as a privacy policy or service conditions. The problem is that

⁹⁶⁵ Draft Recommendation On Self-Regulation, <https://unece.org/> (last visited January 01, 2023).

standards often do not address technological advancements and loopholes.

Few nations have voiced for international agreement to maintain uniformity of the laws governing e-commerce. A model law on e-commerce was adopted by the United Nations Commission on International Trade Legislation in 1996, and it was suggested that member states take this model law into consideration when they passed or amended their own laws. This demonstrated the requirement to harmonise the regulations governing alternatives to paper-based means of information storage and communication. Additionally, United Nations Commission on International Trade Legislation is nearing completion of its Model Law on Electronic Signatures. So far, no concrete steps have been taken to begin the creation of a global convention on e-commerce in general or on specific topics.⁹⁶⁶

A transaction has two actors. One being the merchant who sells goods or services and the consumer who pays for the goods or services. Similarly, self-regulation can be implemented from the merchant side and the consumer side.

Merchants have to act in good faith to gain consumers' trust. In this case, self-control is crucial. Therefore, the process of conducting online transactions, making payments online, transporting items, and resolving complaints must all be self-regulated by merchants. When engaging in self-regulation, retailers must consider a number of factors, including providing accurate contact information, an accurate representation of the products and services, an accurate estimate of any additional costs that may apply, a clear cancellation policy, return options, and refund policies on their websites.⁹⁶⁷ The online retailer is required to take action to safeguard customers'

transactional information, implement a fair process for resolving disputes and coming up with a solution, adopt privacy protection policies, password protection systems, and encryption in accordance with industry norms and legal requirements. Merchants must pay close attention to their marketing practises, including promotions and advertising. They must never intentionally mislead customers in order to gain their personal information.

The merchants' self-regulation model can be strengthened by backing it up with more self-regulation initiatives from the consumers' side. The World Wide Web Consortium has created the software called Privacy Preferences, wherein consumers choose the level of privacy they want by following the principles of notification, control, and choice. Customers could, for example, select to protect as much privacy as possible when using certain websites. Each website would specify its privacy policies and practices. They can allow websites to share information or use information internally. When a user accesses a website that requires more information than the user's privacy preference would permit, the website may either refuse access to the user, ask them to make an exception and accept a lower privacy preference level, or waive their information requirements and let the user access the website on their terms.

A different strategy is supported by Microsoft and Netscape and is known as the Open Profiling Standard. This standard would let customers who want to shop using the internet to create electronic passports that specify the types of sites they want to visit, without mentioning their identities. This strategy would provide consumers with the ability to protect their privacy and limit unwanted marketing.⁹⁶⁸

The most advanced internet technologies and privacy protection rules are found in the United

⁹⁶⁶ Walsh, D., Parisi, J.M. & Passerini, K. Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation. *Electron Commer Res* 17, 185–203 (2017).

⁹⁶⁷ Miller, R. The Need for Self-Regulation and Alternative Dispute Resolution to Moderate Consumer Perceptions of Perceived Risk with Internet Gambling. *UNLV Gaming Research & Review Journal*, 10(1) (2006).

⁹⁶⁸ Zhulei Tang, Yu (Jeffrey) hu & Michael D. smith Gaining Trust Through. Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor, *Journal of Management Information Systems*, 24:4, 153-173, (2008).

States of America. The United States is still worried about enhancing privacy protection and the adoption of sensible measures. The Privacy Act, which is the nation's fundamental privacy law, was passed by the House and the Senate in 1974. While the Act gives federal government agencies the right to acquire and utilise personal data, it also explicitly prohibits them from doing so without the parties' consent. The most significant law addressing difficulties with customer privacy in e-commerce is the Electronic Communications Privacy Act, which Congress passed in 1986.⁹⁶⁹ Self-regulation is used by the e-commerce sector to safeguard customer privacy. The four categories of self-regulatory actions are as follows:

1. Constructive industry guideline: When the Online Privacy Alliance published its online privacy standards, it claimed that its members had given their agreement to adopt and follow its privacy policy, but it did not keep score of how well its members were performing. So keeping a track of e-commerce activities adhering to privacy policy is an important step.
2. E-commerce privacy authentication program: Private businesses commit to e-commerce privacy protection procedures for their customers. These programmes educate businesses about the steps to take in order to protect sensitive data.
3. Technology protection method: It incorporates the component of consumer privacy protection by consumers themselves. Software warns users before they visit websites that may collect personal data. Consumers must then choose whether or not to view the website. As a result, consumers can choose what information is to be collected, get to choose which information is acceptable in advance,

and exclude other information from selection.

4. Safe harbour method: It incorporates both statutory obligations and self-regulation. In addition to the state's data protection laws, it also incorporates e-commerce privacy protection guidelines issued by specific online service providers.

The Federal Trade Commission in the United States framed rules for fair information practices, depending on self-regulation by setting privacy standards, and requiring businesses to establish the following privacy policies:

1. To notify the consumers as to how disclosure of information will be used
2. To take consent by opting in or out of providing information in return for benefits
3. To enable users to check accuracy from combining data from various sources
4. By providing integrated protection from theft or tampering
5. To enforce only credible means of using the agreed data

The US widely prefers industry self-regulation to protect e-commerce consumer privacy. However, domestic industry self-regulation has a limited impact, and a push for legislation to protect online shoppers' privacy has emerged. The US government continues to insist that internet service providers should deal with the issue. Because of the fast development of e-commerce, the US has not passed any comprehensive and systemic federal legislation to self-regulate the right to privacy of e-commerce consumers. It is concerned that hasty legislation may impede the growth of internet commerce.

United States citizens have played their role as self-regulating consumers too. When using an e-commerce marketplace, consumers run into the issue of having no control over the access, collection, use, and disclosure of their personal information. Customers' potential danger of

⁹⁶⁹ Mark E. Budnitz, Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate, 49 S. C. L. REV. 847 (1998).

having their privacy rights violated when conducting electronic transactions is increased because they don't have control over their information. Consumers' reluctance to engage in e-commerce transactions is due to privacy concerns. People desire legislative control over privacy invasions, and in the absence of such legislative controls, customers often use self-regulatory mechanisms to safeguard their privacy in online transactions. Americans have taken efforts to preserve their privacy, such as forgoing online shopping or asking businesses to delete their personal data from databases. Many Americans, because of privacy concerns, chose not to register on an e-commerce website or went against visiting an e-commerce website.

In India, we don't have specific norms to self-regulate private and crucial information of consumers by the e-commerce platforms. But India has recognised that issues regarding privacy theft are prevalent on online commerce platforms. Hence, India has taken the initiative to undertake self-regulatory methods to tackle the problem of privacy theft. Deputy Director of the Bureau of Indian Standards (BIS), Parul Gupta, made the following remarks during the Internet Commerce Summit 2022. ⁹⁷⁰India's e-commerce business is growing rapidly, placing it at around USD 50 billion in 2022. In order to create standards with the goal of self-regulation for managing online reviews, BIS will work with stakeholders in the e-commerce industry. By establishing standards, parties would be able to conduct business of quality goods and services, anywhere and anytime. As part of the government's attempts to fight bogus reviews, BIS has developed standards for e-commerce businesses, travel portals, and food delivery platforms that publish consumer evaluations online. Both solicited and unsolicited reviews have steadily increased over the past few years, influencing customer buying

decisions. They are to be taken into consideration." So, the goal is to track both solicited and unsolicited opinions regarding their products from the makers themselves. Fake reviews can misguide consumers into buying products. Such products would be detrimental to consumer's trust with the e-commerce sector. Therefore, e-commerce must make efforts to identify and remove fake reviews from their platform. Genuine reviews from certified buyers and genuine description from certified sellers should be promoted in order to strengthen trust among consumers. However, this has more to do with quality of products than protection of consumers' privacy.

The Parliamentary Standing Committee on Commerce, referred to as the 'committee' in this paper, has made the decision to look into matters pertaining to the promotion and regulation of e-commerce in India as well as to address the regulatory problems affecting the e-commerce sector.⁹⁷¹

The committee has urged online retailers to sign up with the Department for Promotion of Industry and Internal Trade (DPIIT). Every e-commerce firm must register with DPIIT. The Consumer Protection (E-commerce) Rules 2020, which are draft rules, encourage e-commerce businesses to register with the DPIIT. The committee will also simplify the registration process to encourage more e-commerce entities to register with it. Here again, the initiatives are aimed at encouraging more businesses online but not much to protect consumers' data privacy. The registration will obviously contribute to gain consumers' trust. Consumers trust a registered e-commerce platform more, since compliance to privacy protection regulation will be strictly adhered to by such entities.

More obligations stated under the draft rules make e-commerce transactions accountable

⁹⁷⁰ Indiaretailing Bureau, (2022) *India's standard body bis to engage e-commerce players for self-regulation*, *IndiaRetailing.com*. Available at: <https://www.indiaretailing.com/2022/12/14/big-grid/indias-standard-body-bis-to-engage-e-commerce-players-for-self-regulation/> (Accessed: January 8, 2023).

⁹⁷¹ Jayshree Navin Chandra and Nitika Bakshi (2022) *E-commerce in India: Regulatory framework update*, *Live Law*. Live Law. Available at: <https://www.livelaw.in/law-firms/law-firm-articles-/e-commerce-dpiit-fdi-policy-consumer-protection-e-commerce-rules-213461> (Accessed: January 8, 2023).

vis-à-vis data privacy. The proposed regulations provide that no e-commerce business may reveal any consumer information to anyone besides the customer without the specific and affirmative consent of that customer. Such an entity shall not, including through pre-ticked boxes, automatically record such permission. The absence of a policy and regulatory framework surrounding the usage of data alarmed the committee. The committee suggested that the personal data protection law be passed right away and that precise rules for the use and sharing of data produced by e-commerce platforms be created and put into place as soon as possible.

The Competition Commission of India has recommended self-regulatory guidelines for the platforms of online markets in order to guarantee openness, promote competition, and enhance information symmetry.⁹⁷² In order to protect users' private information, e-commerce platforms must self-regulate by establishing a clear and transparent policy governing the data collected on e-commerce websites and describing how the platform will use this data. Mention the possible or actual sharing of this data with affiliates or other parties. Describe clear and transparent privacy protection policies for customers. For the sake of maintaining the privacy of consumers, such policies shouldn't be arbitrary or discriminatory. The e-commerce website must notify the concerned website users of any planned modifications or revisions to the terms and conditions of a contract, which includes element of privacy. We can therefore relate to the fact that India has recognised the need for privacy protection on e-commerce platforms and is actively trying to put better self-regulation norms into place to safeguard the private information of the general public who utilise e-commerce platforms.

Conclusion

⁹⁷² NewIndianXpress (2020) *CCI asks e-commerce firms to increase transparency*, *The New Indian Express*. The New Indian Express. Available at: <https://www.newindianexpress.com/business/2020/jan/09/cci-asks-e-com-firms-to-increase-transparency-2087187.html> (Accessed: January 8, 2023).

Proper implementation of merchant self-regulation in e-commerce enterprises to protect data privacy on the internet will help in significantly raising the consumers' trust in e-commerce transactions. Some countries have created standardised rules governing acquisition, storage, and use of consumers' personal data by businesses. Additionally, businesses actively create and incorporate privacy protocols into each website's code of practice. It is the duty of consumers to exercise self-control on their end as well. United States of America and European Union have distinct approaches to such regulations. To gain consumer confidence in e-commerce transactions, merchants in the US must develop a model for self-regulation while the European Union emphasises the state's role through judicial rules to protect consumers' data in e-commerce transactions.

Without the involvement of the state, which creates regulations and informs customers about transaction safety, self-regulation cannot function. The quality of self-regulator, a crucial factor, must also be ensured for self-regulation to function well. The merchants need to have extensive knowledge of the regulatory sector. They must have a thorough knowledge of the sector and how it relates to other connected sectors. Besides demonstrating impartiality, the merchants need to be innovative to handle challenging issues facing the sector. To improve consumer behaviour and the state of the e-commerce transaction system, merchants must comprehend and put into practice 'responsibility'. The concept of merchants' accountability for consumer issues can be broken down into two: information accountability and safety accountability. Website certifications and privacy seals from trusted third parties like TRUST-Arc or BBB-online are also means of protecting privacy and creating trust of consumers.

References

Journals

- Abdul Halim Barkatullah, Djumadi, Does self-regulation provide legal protection and security to e-commerce consumers? *Electronic Commerce Research and Applications*, 30, 94 – 101, (2018)
- Walsh, D., Parisi, J.M. & Passerini, K. Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation. *Electronic Commerce Res* 17, 185–203 (2017).
- Miller, R. The Need for Self-Regulation and Alternative Dispute Resolution to Moderate Consumer Perceptions of Perceived Risk with Internet Gambling. *UNLV Gaming Research & Review Journal*, 10(1) (2006).
- Zhulei Tang, Yu (Jeffrey) hu & Michael D. smith Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor, *Journal of Management Information Systems*, 24:4, 153-173, (2008).
- Mark E. Budnitz, Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate, 49 S. C. L. REV. 847 (1998).
- NewIndianXpress (2020) CCI asks e-commerce firms to increase transparency, *The New Indian Express*. The New Indian Express. Available at: <https://www.newindianexpress.com/business/2020/jan/09/cci-asks-e-com-firms-to-increase-transparency-2087187.html>

Online sources

- Draft Recommendation On Self-Regulation, <https://unece.org/>
- Indiaretailing Bureau, (2022) India's standard body bis to engage e-commerce players for self-regulation, *IndiaRetailing.com*. Available at: <https://www.indiaretailing.com/2022/12/14/big-grid/indias-standard-body-bis-to-engage-e-commerce-players-for-self-regulation/>
- Jayshree Navin Chandra and Nitika Bakshi (2022) E-commerce in India: Regulatory framework update, *Live Law*. Live Law. Available at: <https://www.livelaw.in/law-firms/law-firm-articles-/e-commerce-dpiit-fdi-policy-consumer-protection-e-commerce-rules-213461>