



## E-COMMERCE AND PRIVACY ISSUES

SALONI SRIVASTAVA<sup>1</sup>, DR. SHOBHNA JEET<sup>2</sup>

<sup>1</sup>Research Scholar, School of Legal Studies, KR Mangalam University

<sup>2</sup>Associate Professor, School of Legal Studies, KR Mangalam University, Sohna-Gurugram

### **ABSTRACT**

*The utilization of digital platforms for trading goods and services is progressively gaining global traction. Presently, numerous businesses are embracing e-commerce as a means to enhance the profitability of their offerings. The internet serves as a crucial avenue for consumers to procure goods and services and facilitates convenient payment methods. Ensuring the security of online business operations is imperative for achieving success. Thus, the research seeks to examine and address diverse privacy and security concerns within the e-commerce domain. The study reveals a spectrum of causes responsible for security breaches that jeopardize the safety of e-commerce activities. Furthermore, the investigation highlights a variety of measures that enterprises can implement to counteract the escalating threats posed to the security of web-based businesses. Discussions regarding privacy and security concerns in the realm of Information Sciences and data privacy have gained significant attention among users. E-commerce, an integral part of Information Science, is not exempt from the challenges posed by data privacy issues and security threats. Without addressing these concerns, users are unlikely to place their trust in, visit, or conduct transactions on E-commerce platforms. Ensuring user privacy online stands as a paramount concern for E-commerce. The utilization of technical strategies like cookies and data capture has long fuelled privacy concerns. These practices of data mining infringe upon users' privacy within the online realm. E-commerce security pertains to safeguarding the assets of e-commerce against unauthorized access, manipulation, use, or destruction. While E-commerce presents significant opportunities for the banking sector, it concurrently introduces a range of fresh risks and susceptibilities, particularly concerning security threats propagated over the internet.*

**Keywords:** Data protection, E-commerce, Data Privacy, Security Threats

### **INTRODUCTION**

E-commerce, also known as electronic commerce, refers to the process of buying and selling goods over the Internet. This encompasses various transactions, such as purchasing clothing, footwear, and other items through online platforms. Essentially, e-commerce involves businesses and consumers engaging in electronic exchanges to acquire and vend products. This domain encompasses a range of activities, including online marketing, supply chain operations, digital transactions, mobile advertising, and the electronic transfer of data. These digital pathways facilitate business operations and expansion. In India, the increased penetration of the Internet and higher disposable incomes have sparked a significant shift in shopping behaviour. People across diverse segments are utilizing smartphones to make purchases. E-commerce has effectively eliminated the constraints of time and distance in trading, offering a seamless solution devoid of persistent challenges. In essence, it has become a boon for businesses, furnishing them with an excellent platform to showcase their products online, thereby fostering non-uniform growth. Simultaneously, it has empowered consumers by simplifying the process of finding desired products without the need for physical exertion. Through a mere click, the product becomes accessible. The advent of e-commerce has completely revolutionized the traditional methods of buying and selling, bringing about a profound transformation in the realm of Internet commerce.

Commerce involves conducting business operations over the internet through web-based platforms. E-commerce has gained immense popularity in recent times, but it has also brought to light various privacy concerns. If these issues are not effectively addressed, users might opt out of engaging in

online transactions.<sup>1</sup> Business proprietors in the e-commerce domain sometimes exploit users' privacy to foster business growth. Different authors present varying interpretations of privacy. For instance, Etzioni defines privacy as measures that are considered socially unacceptable or unfeasible.<sup>2</sup> Davies characterizes privacy as a right that often goes unutilized.<sup>3</sup> Experience demonstrates that users are apprehensive about unauthorized access to their personal data. They are reluctant to allow the reuse or sale of their personal information for commercial purposes. Presently, online service providers emphasize their privacy policies.<sup>4</sup> The expansion and trustworthiness of E-commerce enterprises heavily rely on the security and privacy policies of their websites. Establishing user trust is a pivotal factor for the advancement of E-commerce.<sup>5,6</sup> To uphold privacy in E-commerce, a comprehensive and secure system is imperative.<sup>7</sup> Despite the enhanced security and convenience of online payment systems, users still exhibit reservations when it comes to E-commerce transactions.<sup>8</sup>

#### **The origin and evolution of E-commerce:**

E-commerce initially emerged during the 1960s with the commencement of data transmission over the internet. This marked the utilization of Electronic Data Interchange (EDI) technology, enabling the transfer of files and documents via the internet for business purposes. The progression continued, and in the 1990s, online shopping businesses began to take shape, experiencing exponential growth thereafter. This growth alleviated the constraints of time and distance for buyers. With the subsequent advent of smartphones, purchasing transformed into a matter of a single click, enabling individuals to procure their desired items conveniently, anytime and anywhere, with just a prerequisite of an internet connection. This convenience resembles a thread connecting buyers to the virtual realm of online shopping stores, where millions of products can be perused on the screens of their smartphones.

#### **E-commerce can be categorised in:**

- i. *Business to Consumer (B2C)*: In this type of electronic commerce, businesses sell their products to customers through online platforms. Customers search for desired items, add them to the cart, and make purchases using online payment methods like credit/debit cards or net banking. Amazon and Flipkart are prime examples of B2C e-commerce.
- ii. *Consumer to Business (C2B)*: This involves consumers selling products to businesses via the internet. An instance is participating in paid surveys about a company's products.
- iii. *Business to Business (B2B)*: This entails online buying and selling between two businesses. For instance, companies providing hosting services, such as GO Daddy, offer domains and hosting solutions to other companies.
- iv. *Consumer to Consumer (C2C)*: C2C e-commerce involves individuals selling items they no longer need to others over the internet. OLX is a prominent illustration, providing a platform

<sup>1</sup> Budak C, Goel S, Rao J, Zervas G (2016) Understanding emerging threats to online advertising. ACM Conference on Economics and Computation pp: 561-578

<sup>2</sup> Lee I (2016) User Privacy Concerns for E-Commerce. IGI Global: Encyclopaedia of E-Commerce Development, Implementation, and Management pp: 1780-1787.

<sup>3</sup> Ackerman MS (2004) Privacy in pervasive environments: next generation labelling protocols. Personal and Ubiquitous Computing 8: 430-439.

<sup>4</sup> Ackerman MS, Davis TD (2003) Privacy and security issues in e-commerce. New economy handbook pp: 911-930.

<sup>5</sup> Smith R, Shao J (2007) Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7: 89-116.

<sup>6</sup> Corbitt BJ, Thanasankit T, Yi H (2003) Trust and e-commerce: a study of consumer perceptions. Electronic commerce research and applications 2: 203-215.

<sup>7</sup> Lau RY (2007) Towards a web services and intelligent agents-based negotiation system for B2B eCommerce. Electronic Commerce Research and Applications 6: 260-273.

<sup>8</sup> Castañeda JA, Montoso FJ, Luque T (2007) The dimensionality of customer privacy concern on the internet. Online Information Review 31: 420-439.



for users to list items they want to sell, with interested buyers directly contacting the sellers through the provided contact information.

#### Characteristics of E-Commerce:

- i. *Global Accessibility*: The foremost and most advantageous characteristic of E-commerce is its global accessibility. Irrespective of location, anyone can purchase desired products from anywhere in the world. No country is beyond reach, and products selected are conveniently delivered to the provided address within specified timeframes. Therefore, geographical barriers hold no significance - your chosen product will reach you, regardless of your location.
- ii. *Omnipresence or Ubiquity*: E-commerce's foundation in internet technology allows for effortless and efficient use. With just an internet connection, commonly via Wi-Fi hotspots, you can navigate through desired items from the comfort of your home. Unlike traditional markets with fixed operating hours, e-commerce transcends time restrictions. Online stores are open around the clock, 24/7, offering unparalleled convenience and accessibility.
- iii. *Information Density*: A distinctive strength of E-commerce is its exceptional information density. This means that using E-commerce reduces costs related to data storage, processes, and communication. It provides a wealth of accurate information at no additional expense, often presented in a comprehensive manner.
- iv. *Interactivity*: A prominent and pivotal aspect of E-commerce is its ability to offer genuine interactivity with consumers. This level of interactivity ensures transparency throughout processes, such as tracking shipments and deliveries post-order. Establishing this level of trust through interaction contributes to cultivating long-term customer relationships.
- v. *Universal Standardization*: E-commerce's perpetuity can be attributed to its universal standardization. Individuals, governmental bodies, and businesses alike adhere to the same standards, utilizing the same media (internet) and technical norms to access E-commerce platforms. A universal standard ensures consistent and straightforward user experiences, wherein everyone must register, creating a personalized account accessed through a unique username and password.

In recent times, India has experienced remarkable growth within the realm of e-commerce, boasting a user base of approximately 300 million internet users. This surge has been particularly prominent in sectors such as e-retail, electronic goods, fashion, and home appliances. This surge has not only created numerous opportunities for the younger generation but has also positioned them as leading entrepreneurs, thereby generating a substantial number of job opportunities. Looking ahead, over the next five years, there exists the potential for a shift toward utilizing social media platforms for purchasing and selling goods. Furthermore, there is a possibility of the delivery system evolving into a more sophisticated structure, incorporating technologies like quad-copters or drones. The integration of artificial intelligence is expected to enhance the accuracy and efficiency of customer interactions, with robots being capable of comprehensively addressing your queries.<sup>9</sup>

#### The Significance of Protecting Data Privacy in the Digital Era


In the contemporary digital era, the value of our personal information has escalated substantially. The advent of social media, e-commerce, and online banking has led us to share a greater volume of personal data than ever previously. While these technological advancements have undoubtedly enhanced our daily lives, they have concurrently introduced novel threats to both our privacy and security. This article will delve into the critical importance of data privacy and provide insights into safeguarding oneself in the digital age.

##### *The Relevance of Data Privacy*

Our personal information holds multifaceted value. Advertisers exploit it to tailor personalized advertisements, while social media platforms scrutinize our behaviours to deliver more captivating content. Yet, the jeopardy ensues when unauthorized parties gain access to our personal data, wielding it for malicious intentions. This data can be exploited by hackers for identity theft, unauthorized access to financial accounts, and even extortion. Beyond these risks, ethical concerns

---

<sup>9</sup> <https://www.maxvisionsolutions.com/blog/an-introduction-to-ecommerce-growth-of-e-commerce-in-india>



persist regarding how companies harness our personal data. The perpetual surveillance and monitoring experienced online make many individuals uneasy. Maintaining data privacy holds significance in the era of digital advancement. As our online sharing of personal information intensifies, it's crucial to acknowledge the associated hazards and proactively safeguard our interests. Employing robust passwords, exercising prudence when divulging personal details, and consistently monitoring our accounts are essential measures to mitigate the likelihood of succumbing to cyber threats.<sup>10</sup>

#### *Social and Business Aspects*

Privacy holds delicate significance within the realm of business. We address privacy from both a technical perspective and through considerations of consumers' apprehensions. Employing digital systems and novel computational methods for data mining facilitates data capture. E-commerce platforms amass substantial quantities of data pertaining to customer preferences, purchasing trends, and search behaviour on a large scale. Business analysts leverage this data to enhance customer experiences through personalization and elevate the performance of the e-commerce site.<sup>11</sup>

#### **Privacy in respect of E-commerce**

Privacy concerns are a significant matter in the domain of electronic commerce, regardless of the source under examination. Culnan asserted that privacy apprehensions were a key factor deterring people from going online and even led to instances of providing false information on the internet.<sup>12</sup> In reality, only a minority of consumers feel they have substantial control over how personal information disclosed online is utilized or sold by businesses.<sup>13</sup> The confluence of existing business practices, consumer anxieties, and media influences has contributed to making privacy a formidable challenge for electronic commerce. Differing perspectives exist on privacy - some view it as an intrinsic right while others see it as a negotiable commodity. Alongside "privacy," several concepts including digital persona, notice, identification, choice, authentication, pseudonymity, anonymity, and trust are also vital concerns in the realm of e-commerce that need addressing. E-commerce platforms have the potential to amass extensive data about consumers, encompassing personal preferences, shopping behaviours, information search patterns, and more, especially when data is aggregated across various sites. Collecting this data has become easier than ever, and searching through it has also been streamlined.<sup>14</sup> Novel computational techniques enable data mining to scrutinize consumers' purchasing patterns and personal trends almost instantaneously. Consumers express dual privacy concerns. Firstly, they worry about the risk of secondary usage—where their personal data is reused for unrelated purposes without consent, such as sharing with third parties not involved in the original transaction. Secondly, unauthorized access to personal data due to security breaches or inadequate internal controls is a significant concern.<sup>15</sup>

As we witness the transition to a digital world propelled by e-commerce, it's evident that this shift encompasses more than just buying and selling; it now encapsulates nearly every facet of life. Virtually everything is available at the click of a button. However, this technological advancement is a double-edged sword, offering convenience but also introducing the constant threat of cybercrimes. Cybercrimes, ranging from violating individual privacy to jeopardizing national security, pose real and significant risks. Privacy concerns have grown further as our lives are increasingly exposed through

---

<sup>10</sup> <https://www.linkedin.com/pulse/importance-data-privacy-digital-age-thetechmarketer>


<sup>11</sup> Muneer, Asia & Razzaq, Samreen & Farooq, Zaineb. (2018). Data Privacy Issues and Possible Solutions in E-commerce. *Journal of Accounting & Marketing*. 07. 10.4172/2168-9601.1000294.

<sup>12</sup> Culnan, Mary J., and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1) : 104-115.

<sup>13</sup> Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37

<sup>14</sup> Winner, D. 2002. Making Your Network Safe for Databases. SANS Information Security Reading Room, July 21, 2002.

<sup>15</sup> Dhillon, Gurpreet S., and Trevort T. Moores. 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14 (4) : 33-37



social media. Determining what and how much to share has become a pivotal question. Many company websites aim to create user profiles to monitor preferences and interests, often collecting more data than necessary or relevant. Online security challenges are pervasive and traverse borders, presenting an undisputed cross-border nature. The interconnectedness of systems through the internet exposes them to potential targeting, leading to data tampering. Websites offering online services are vulnerable to attacks that could result in site blockages or denial of service. Unauthorized access can lead to unauthorized modification or alteration, jeopardizing data and causing financial loss. Incidents like these erode trust in networking and online systems, ultimately impacting the confidence of the public. With the escalating trend of e-commerce, such incidents foster distrust in networking and online systems. It's imperative to protect systems and networks, as the repercussions extend to critical infrastructure such as power grids, LAN networks, and organizational security systems. Such vulnerabilities can lead to financial losses, human resource constraints, and a decline in public confidence.

### **Privacy & legal regimes of e-commerce in India**

#### *i. Information Technology Act, 2000*

In India, the Government enacted the Information Technology Act, 2000 (IT Act) in June 2000 to address e-commerce issues and establish regulations. The IT Act, influenced by the UNCITRAL model e-commerce Act, aims to foster consistent legal recognition for e-transactions. The UN model outlines the fundamental concepts of electronic communication, electronic signatures, and documents. The Act emphasizes the equivalence of electronic signatures and records to their traditional counterparts. Consequently, amendments were made to various laws, including the *Indian Penal Code, 1860*, *The Indian Evidence Act, 1872*, *Bankers' Books Evidence Act, 1891*, and *Reserve Bank of India Act, 1934*. Rooted in the UN e-commerce law framework, the IT Act's preamble underscores its purpose "to provide legal recognition for transactions carried out by the means of electronic communication, commonly referred to as 'electronic commerce' which involves the use of alternative to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies".<sup>16</sup> Additionally, the Act focuses on securing electronic records and digital signatures. Defined in Section 2, "cyber security" refers to "Protecting information, devices, equipment, computer resources, computer devices and information stored there in from an authorised assess, use, disclosure, disruption, modification or destruction."<sup>17</sup> While the IT Act addresses certain cybercrimes explicitly, it does not cover others such as cyber stalking, harassment, or defamation. It addresses unauthorized access to computer systems through sections on cyber contraventions.

Sections 65 to 78 of the IT Act delineate offences and corresponding penalties for specified cybercrimes. The Act also deals with civil offences and the associated penalties. Although the IT Act is instrumental in building an e-commerce and e-governance framework, it has limitations, and its goal is to foster confidence that cyber wrongdoings will face consequences.

#### *ii. The Payment and Settlement Service Act, 2007*

It governs various payment systems in India, including RTGS, ECS Credit, ECS Debit, credit and debit cards, NEFT, Immediate Payment Service, and UPI. Regulated by the RBI, this Act defines payment systems as mechanisms facilitating transactions between payers and beneficiaries, encompassing clearing, payment, settlement services, and related operations, excluding stock exchanges.<sup>18</sup>

#### *iii. National E-Commerce Policy*

The draft of National E-Commerce Policy released by the Department for Promotion of Industry and Internal Trade under the Ministry of Commerce and Industry aims to address key e-commerce issues, such as data, infrastructure, marketplaces, regulation, domestic digital economy, and export

---

<sup>16</sup> The IT Act, 2000, Preamble

<sup>17</sup> The IT Act, 2000, Sec. 2(nb)

<sup>18</sup> The PSS Act, 2007 Sec. 2(1)(i).



promotion. While this draft policy has not yet been enacted, it underscores the ongoing efforts to shape a comprehensive framework for e-commerce in India.

### CONCLUSION

With the growing trend of e-commerce, threats, online fraud, hacking, online fraud and cyberwar as well as illegal activities appear at the same time as the trend of e-commerce. developing death. To limit this growing threat and only attack the root of the problem, many laws have come into force in many different countries. As we can see, there are some slight differences between the laws and policies of different countries, but there is one major similarity: the object and purpose of each law is common; protect the interests of online users, provide them with a safe environment to access the digital world, build trust in the digital market by feeling safe without worrying about rights their privacy. Similarly, India has also passed its own law based on the UNCITRAL model for the legal recognition of e-commerce as mentioned above. Regarding the granting of legal status to electronic signatures and records, although efforts have been made to provide frameworks for this and overcome some cases of abuse of the technology, it also has some limitations. Some say it's an ineffective law; there are some areas that need attention that he is lacking. India has no specific legislation regarding privacy laws, although concerns about privacy are at a peak. It is also a barrier to e-commerce as it leads to the loss of significant foreign investment and other business opportunities. India is the host country and largest data outsourcing platform. An effective and well-constructed solution is needed to combat these crimes. It must do more to ensure the sustainability of specific and effective data protection laws. In the era of globalization and e-commerce, technology plays an important role in the development of the economy. Thanks to the global information highways, the concept of information has been given a new and different dimension. E-commerce has given wings to this new revolution by changing the business model. For 20 years, e-commerce has established itself as a new dimension in the economic world, where information is considered the biggest and most important asset. India, the second most populous country in the world and having a young and consumer-oriented society, is becoming a veritable treasure trove of information. In India, the e-commerce market has experienced steady growth in recent years. secure India's cyberspace and improve the business environment by enabling quick and efficient access to government services through online portals. All of this means that India is a remarkable part of the global digital revolution. As digital commerce becomes an integral part of modern life, it is important to think about the issues associated with it. Comprehensive legislation is needed to address the privacy issues that are central to today's times. Creating a privacy policy is a necessity at this point The website of the relevant company is responsible for notifying customers of their privacy policy and any related changes. Customers should be selective by allowing them to change their own privacy settings to control how much data is collected and used. The computer law should include a list of major crimes that have not yet been included in the law, and should also increase the level of punishment provided for in the law. Without a doubt, we have taken an important step towards digital globalization, starting to digitize at a fundamental level, becoming part of e-commerce and taking it to the next level. new high. But at the same time, it requires a solid security system backed by network law, privacy policy, security policy and network technology to provide a safe environment for users; consumers, organizations participate in e-commerce in different stages such as electronic transactions, buying, selling, providing or receiving services, etc.