JOURNAL OF NORTHEASTERN UNIVERSITY

Volume 25 Issue 04, 2022 ISSN: 1005-3026 https://dbdxxb.cn/ Original Research Paper

# RIGHT TO PRIVACY IN THE LIGHT OF DATA MONETISATION BY E-COMMERCE COMPANIES: ISSUES AND CHALLENGES WITH RESPECT TO INDIA

**Anushtha Saxena**

Assistant Professor (Law), Chotanagpur Law College, Ranchi University, Ranchi, Jharkhand.

## 1.1 ABSTRACT

In Justice K.S. Puttaswamy (Retd) and Another v. Union of India,[1] the Supreme Court of India recognised the Right to Privacy as a guaranteed Fundamental Right and one of the facets of Article 21 of the Constitution of India. The court took cognisance that the right to privacy is violated in varied ways and circumstances. One such violation mostly goes unnoticed when committed by e-commerce companies. To understand their customers, e-commerce companies collect their information in the form of their choices, likes, dislikes, etc. This collected information is called Data. Companies use the collected data to create new business opportunities and increase revenue. This process is called Data monetisation and can be done directly or indirectly. Companies nowadays have access to the vast amount of data that e-commerce companies use to generate profits in the market. Data collected, stored and analysed is used to target customers to know the prevailing market needs and how business can be expanded or also by selling the data collected to third parties in raw form.

In the absence of any concrete legal framework for data protection from these e-commerce companies in India, these companies operate of their own free will and collect data from vast volumes of Indian consumers. However, this practice leads to latent violations of an individual's "right to privacy". Consumers, while buying products and services from e-commerce companies, knowingly or unknowingly, give a lot of data to the companies which they use to collect personal information, financial information, their choices, preferences, etc., so that this data can further be collected, stored, analysed by e-commerce companies to monetise their business activities. They deliver innovative products to their consumers through data monetisation and gain revenue.

Therefore, this paper explores the concept of individuals' right to privacy in light of data monetisation by e-commerce companies and examines how data monetisation infringes individuals' right to privacy. The present legislation in India does not give vital protection to the e-consumers concerning privacy matters in online transactions. The right to privacy of e-consumers should be protected in the light of Fundamental rights being guaranteed to them in the Constitution of India under Article 21.

**Keywords**: Fundamental Rights, Privacy, Data monetisation, e-commerce companies.

## 1.2 Introduction

In India, e-commerce has developed significantly alongside the increasing number of internet and social media users. The use of the internet has changed the mindsets of India's population, and now people have switched to online shopping as this mode is too convenient in today's

[1] (2017) 10 SCC 1

**Submitted**: 15/09/2022 **Accepted**: 17/11/2022

time when everyone is busy with their hectic life schedules. E-commerce provides various services and goods to consumers. E-commerce has multiple advantages associated with it, for example, convenience, time-consuming, comfort, flexibility, etc.-commerce enables consumers to get the products ordered from the websites quickly. It has transformed businesses not only in India but also globally. It is a new economy for the companies in India, which has also played a vital role in revenue generation and employment generation. The younger generations especially are valuable consumers in India and worldwide in an online shopping environment. The growth of e-commerce is also increasing because of its significant discounts and sales (IBEF, 2016). For example, famous e-commerce players like Flipkart, Amazon, Myntra, Ajio, Tata Cliq etc., offer discounts, bumper sales offers with attractive taglines like "Big Billion Day Sale", etc., are increasing their customer base. There are many different models that exist in e-commerce, like business-to-consumer, business-to-business, business-to-government, consumer-to-consumer, and consumer-to-business. For other models of e-commerce to flourish in today's time, trust is most important, and it was also embodied by the Organization for Economic Development (OECD)'s that trust is one of the severe themes for the growth of electronic commerce (Branscum,2000). According to the IBEF report and Grant Thornton reports (IBEF, 2016), the Indian e-commerce market is expected to reach US$ 350 billion in 2030 from US$ 188 billion in 2025, and this growth will be seen due to an enormous increase in smartphones, internet and digital India initiative taken by the Government of India. This paper focuses mainly on the legal issues of infringement of privacy by e-commerce companies in the light of data monetisation. Undoubtedly, e-commerce companies are making people's lives much more accessible with just one click away. E-commerce takes place intra-border, i.e., domestic route, or international transactions, i.e., cross-border route.

**Right to Privacy**

Privacy is a principle of common law that was recognised much before any constitution of a state. Instead, it was recognised as an international human right beforehand. Privacy means a person will have full protection concerning his person and property (Cranor, 2017). The law meets the demands of society by recognising political, social, and economic rights from time to time. In the old times, the only remedy for interference in life and property was given by the law. At that time, "right to life" gave protection from the battery, and liberty meant freedom from restraint. Right to Property meant protection of land and cattle. But after some time, more legal rights were given, like the right to be let alone, the right to enjoy life, liberty, etc. In the article 'On Privacy', the author E. van den Haag defines privacy as something that entitles people to exclude other people from their realm and not to allow them to watch, invade, etc., one's private life (Bélanger & Crossler, 2011).

The notion of the right to privacy is applied in diverse fields, and with the information technology and rise in electronic media, this right has become a key right in these areas. Despite numerous attempts, privacy cannot be defined as it has no clear-cut edges. Nowadays, we hear the term "Internet privacy" everywhere. The word "Internet privacy" means information about an individual and their concerns regarding regulatory measures and profiling when it goes on

the internet (Cranor, L. F. 1999). In this digitised age, communications are digital, and information is stored everywhere, thus creating information privacy by merging personal communication privacy and data privacy merging. Thus, data can now be collected, stored, and analysed quicker and in mass volumes, even without an individual's consent or knowledge in the information age era. (Kenneth Cukier, 2013).

In this article, the researcher has thrown light upon the main issue and challenge of infringement of privacy in the light of the data of individuals used by the e-commerce companies in the process of data monetisation. In this age of big data, companies collect data to generate internal and external value through techniques and strategies that create a massive volume of data. The term data monetisation is not a new term. Rather it was seen a few decades ago in the cases of Tesco and Nielsen, wherein these firms played a global role and exchanged data for marker research and leading to data monetisation. According to Gartner Report, Gartner Institute, "data monetisation means data for quantifiable economic benefit". In general, data monetisation simply means generating revenue from the sources available and streamlining the data to store, analyse, disseminate, etc. It is a process that uses technologies and businesses to create value (Spiekermann, M.,2019).

**1.3 Survey of Literature**

India is on the lines of becoming one of the leading countries in the growth of the digital economy there are also threats related to the digital economy, which India has already started facing being legal issues or ethical issues (Electronic Frontier Foundation, 2021). The rapid increase in the digital economy leading to data protection and privacy issues are the major concerns for any country these days. The growth of e-commerce companies has also raised various questions related to data protection and the privacy of data of the consumers. The increase in the technologies today has increased the process of data monetisation because there is sharing of data directly or indirectly to create new data, sell data to generate revenue and provide better services to the consumers. Various techniques, for example, profile algorithms, are used to mine data in order to further their interests. These techniques enable e-commerce companies to generate data related to consumers' choices, preferences, habits, etc., to sell more and more of their goods and services (Cranor, 2017).

The main focus is on the four aspects, data collection, data storage, data analysis, and the use of the data. The companies gather information with the help of these major four aspects to predict future insights of companies, basically called the "autonomy trap" (Anirudh Burman, 2020). For example, a boy Alice is looking for smartwatches from various stores online. The search engine and e-commerce websites are recording their data and using it for their monetisation purposes. This can be avoided if there are tools related to security, anonymity, autonomy and transparency (Tara J. Radin, 2001).

The data collected by the e-commerce companies has given opportunities to utilise and grow business. There are techniques and benefits of data collection to monetise businesses. Data collection and analyses enable the companies to understand comprehensively the needs of their consumers, what kind of discounts should be given to the consumers to retain them, to give products and services on sale offers, etc. (Edward J. Walters, 2021).

There is a huge increase in the personal data economy of the e-commerce entities by purchasing enormous data of the people through various measures and technologies. Havoc has been created, which is not visible, but the impact can be seen; there is a divide between data protection and the protection of the right to privacy of the individuals.

McKinsey Global Survey report (McKinsey & Company, 2017) has also revealed data analytics used to reveal information from the data gathered to develop new businesses, technologies, innovative ways, etc., to gain and capture a major proportion of the market share globally as well as domestically. According to the report, it is a new concept that is being encouraged in companies to monetise businesses and generate revenue. The role of data analytics is a very important strategy to capture the market as well as the consumer's trust by giving the best services to them.

The paradigm of data exchange is rising, and the world is facing the common problem of data security and protection at the cost of the consumer's privacy and the revelation of their personal information. There is a need to identify the areas so that this issue is tackled and there is some permanent solution. There should be proper legal measures and regulatory mechanisms to enhance security issues with respect to the data and privacy of the individuals. (Mohammad S. Najjar, William Kettinger, 2014). Data is sold by signing contracts between the companies. There are dealers and suppliers who enable them to fulfil these contracts and develop a strong business model. The companies also outsource their data in the process of data monetisation (Joseph Phelps, 2000).

The concept of privacy is not a new concept but with the technological advancements, this concept has touched upon other domains like information and communication technologies. The threats posed by the leakages of data of the individuals in several cases in recent years are making the governments and organisations think if this can be protected and whether constructive steps can be taken to protect the data and privacy of the individuals. If we take the example of India, we have nothing in the present date except the Information Technology Act, 2000, to protect data and privacy. But this Act is also not stringent enough as it has loopholes and lacunae to give robust protection to the citizens concerning their data and privacy. (Dhiraj R. Duraiswamy, 2017).

### 1.4 Methodology

The researcher has adopted a doctrinal method in conducting the research and relied upon credible authorities and secondary sources.

### 1.5 Result and discussion

#### 1.5.1 Data collection and its techniques

E-commerce companies are much more dependent upon the datasets and databases based on which they take decisions in their businesses. There was not much demand for e-commerce companies in traditional times as the internet was not much developed, and only a few people preferred online shopping. At that time, the local markets or the vendors-maintained records of their customers and clients manually only. For example, a bakery starts retaining consumers' behavioural data for one whole year. They collected and maintained a record of purchases throughout the year. However, with time they learned and discovered that the customers

ordered cakes and pastries from the bakery mostly on Christmas. To stimulate interest in the customers to make them buy throughout the year, they tried to improve the overall responses they started giving them more choices, discounts, etc., so that the profits are increased. Information that the companies find is valuable to them as well as to others also.

However, gradually with the increase in internet usage and the growth of e-commerce companies, strategic planning and management also started going change. Nowadays, e-commerce companies are maintaining the database of their customers for better revenue and sales. The e-commerce companies help consumers quickly access websites in the digital world, and transactions easily occur between organisations and individuals. The information is flooded with e-commerce companies, and they know what data is important to them and what is not so important.

Various techniques and methods are applied to collect data, information about consumers, store data, etc., by e-commerce companies. There are various methods of data collection, one such being click-stream data, data pre-processing, etc. The e-commerce entities store this data for further references and usage in their databases. The various methods available for pre-processing include cleaning the data, reduction, which means compression of data by following a specific model, transforming data for further analysis and then integrating the data; lastly, discretization is done in which the data is stored. (Tara J. Radan, 2001)

Data is stored in massive amounts, and then data analysis is performed on the pre-processed data. Data analysis is performed, and later on, data visualisation is also performed to know and understand hidden data patterns. Lastly, data exposition is done in the last stage to get the insights into the data to use for its purposes or to sell the data or trade with a third party for advertisements, etc. (Janice Y Tsai, 2011)

Companies and businesses use this framework to capture data through technologies and artificial intelligence to monetise and exploit data. This helps e-commerce companies to capture visitors' and consumers' habits, preferences, advertisements clicked by the customer, rating of the product by the consumer, etc., and record them for the purpose of utilising and monetising on the basis of the analysis done.

For example, e-commerce companies can determine from a woman's purchasing behaviour and patterns that she was looking for baby-related items. The e-commerce companies will use this information to send advertisements related to baby products and to maintain the long history of their consumers. Companies are targeting and mining data to provide better designs, products, innovations, etc.

Data mining is also done by e-commerce companies to discover patterns and extract valuable information from the data sets by filtering and converting raw data into valuable knowledge (Borgesius, 2015). The process of data mining is applied to the information collected to segregate the valuable data. It is one of the technologies that help in the collection of tools and techniques, and businesses learn from data mining techniques because they believe in informed decisions rather than uninformed decisions. It is the analysis of data collected in huge quantities so as to enable e-commerce companies to improve their businesses. Large-scale businesses use Information technology, artificial intelligence, automated machines, etc., to collect raw data

and later use it for data mining. It is a learning opportunity for e-commerce companies from the data gathered. The process of data mining starts once the opportunities are identified as a new product to be launched, understanding and learning consumer demands, etc. For example, Google knows what the consumers are looking for, and thus, Google sells sponsored links by collecting valuable data. (Maureen K Ohlhausen, Alexander P Okuliar, 2015). Data is at the heart of most companies' core business processes" and this has been proved by the e-commerce companies collecting huge data by various techniques and latest technologies.

The information that will be useful can also be obtained by the e-commerce companies from web usage mining techniques that help record and later analyse the behavioural patterns and profiles of the consumers or visitors. This behavioural analysis enables to know the consumer's preferences, the demand for the product or services, pricing pattern, behaviour, likes, and dislikes, etc., are known to the e-commerce companies.

The market size and growth of the global data market is expected to rise at a frequency of 24.1% by 2027 as per the report by Grand View Research. It is seen how the digital economy has become an integral part of every sector, and e-commerce is not behind. With the digital economy comes the concept of data privacy, the protection of data, data collection, data storage, data localisation, etc. E-commerce companies are using data which has become the new asset in the present times, and data is being used to generate revenue and take the business to another level with the collection of data. This process is called data monetisation. The global market will rise due to big data, big data analytics, advancements in technology, etc. The e-commerce companies make use of data generated and collected to monetise their business and generate revenue and with the help of the latest technologies for designing efficient products and services in such a way that they also reduce costs and provide the best services to the consumers.

Also, various reports have revealed that the data is sold by the data brokers to increase the marketing techniques and create market segments. There is a strong relationship between data markets and capital markets. The personal information is extracted from the online advertisement, etc. s, through cost per click, cost per installation, cost per impression, etc. Data markets and advertisements help collect massive data of consumers and later help in determining price, whereas the consumers do not know anything about their data sharing, transferring and collection with the companies. These practices are not in line with the information-sharing practices, and thereby it is necessary to have regulators regulate and control the use of personal data. Fines and penalties are essential for compliance and sanctions. (France Bélanger & Robert E Crossler, 2011).

It is seen that traditional small businesses and local markets build relationships with the customers over time and learn ways to serve them in a better manner. They keep in mind their needs, preferences and how to do them better. The result is that the small businesses earn loyalty, happy customers as well as profits from their traditional local businesses. However, this is not true for a company running a business on a larger scale, and they do not enjoy the luxury of personal relationships with the customers. They make use of something they have in large quantities, namely the data generated by online shoppers, in order to fully exploit their

businesses and the consumers. The companies are trying to build a business based on customer relationships.

However, for e-commerce companies, it is not possible to maintain records manually and therefore, they go for data warehousing techniques to exploit and make use of data generated to know the products and any innovations to be made in it, marketing of those products, etc.

**1.5.1.2 Data Monetisation by e-commerce companies and its techniques**

Monetisation is not a new term but these days in every field we hear this term very frequently. Monetisation plays a very important role in present times, and it is one of the methods of bringing evolution to businesses. Data monetisation is a process of collecting data directly or indirectly by the application of various techniques as discussed above. In today's digital world, where people are more involved in buying goods and services online, e-commerce companies at the same time, are facing the challenge of converting valuable data into value directly or indirectly. Turning data into profit and helping in decision-making is called the process of data monetisation. By 2026, it is anticipated that the market for data monetisation will have grown to USD 7.47 billion. This idea of data monetisation is gaining popularity as a result of the development of technology, big data, and the Internet of Things.

The e-commerce companies are focussing mainly on cutting costs and improving profit margins. The e-commerce companies, through advertisements, also give insights to the consumers, for example, if a person is looking for a flight for a vacation and there is an advertisement regarding the hotels at that particular place, it is very obvious that the person will be interested in it. The consumers will click on the advertisements, and if the hotels, etc. are available at a cheap price, then it is not a problem for them. Now, this data is stored with the e-commerce companies through advertisements, clicks, etc., and they will try to improve their services based on this data of consumers. The following chart represents the idea and how the process of data monetisation , directly or indirectly is done by the business organisations.

There was a survey conducted by McKinsey Global Survey in 2017(McKinsey, 2017), revealed that the companies are moving towards a business that is data-centred. They are using data and data analytics methods to generate revenue and profits in their businesses. The sales, marketing, research and development practices have changed and transformed due to data analytics. The companies are focussing on automated processes and data-driven culture to experience better growth, innovation, new business models, etc. We are living in the Internet of Things age, and data is the new asset in the economy, accelerating businesses and companies to transform in a different manner. The new oil of the modern digital economy is data.

The process of Data monetisation is increasing because the companies are reaping benefits by spending less money. This is because with the help of emerging technologies vast volume of data is collected, but the storage cost is decreasing as there is an increase in big data analytics, cloud computing, etc.( Russom, Philip, 2011) The e-commerce companies use various types of data like behavioural data, i.e., the experience of consumers with the e-commerce company, for example, free trial version downloads and sign up, etc., Basic data is collected to know the name, and contact details of the consumers, gender, etc. The third type of data that is collected is attitudinal data, i.e., the opinion of the consumers related to the product and service, for example, comments, reviews, ratings, etc. All these data are used by e-commerce companies in order to make appropriate business moves and competition and identify the challenges and opportunities in the market. (Jose Maria Cavanillas, Edward Curry, 2016) .

There are various authors, Najjar and Kettingar, who have highlighted the importance of data monetisation in the present times (Mohammad Najjar, William Kettinger, 2014). They have focussed on analytical knowledge of companies, building data infrastructure and sharing data with third parties who can be suppliers, etc. Other authors, Opher A, Chou A, and Onda A in their article, have explained the emerging data monetisation and the direct benefits gained by the data monetisation (IBM Corporations, 2011) and the company's performance based on the big data monetisation. It offers various opportunities, timely business decisions, etc. (Opher A, Chou A, Onda A, 2016).

### 1.5.2 Infringement of Privacy by E-Commerce Companies

The main question here is whether the process of data monetisation by e-commerce companies is infringing the right to privacy of consumers. Let's first answer the question as to what is Privacy. Privacy is defined by various scholars (Mason, R. O.,1986) in his article, suggested that in the 1980s, the Information Age or the world of technologies would lead to four major issues related to information, i.e., the issue of privacy, the issue of accuracy, the issue of property, and the issue of accessibility (PAPA). It is demonstrated to be precise, especially in the privacy domain, which is the concern of everyone nowadays. Privacy included various parts, one being informational privacy. Controlling access to one's personal information in organisations is a worry shared by all, according to a Pew Internet Project survey. This survey found a breach of privacy of nearly about 63 per cent. The companies in this survey indicated that they spent maximum time reacting to these breaches rather than preventing them (Joseph S, Fulda, 2000). Therefore, information privacy is studied by many researchers in the field of law, management, and other areas. Privacy also means human rights in various terms and

contexts. The privacy of an individual, personal behaviour privacy, personal communication privacy, and personal data privacy are some of the characteristics of privacy that academic Clarke described in his work. (DeCew, Judith Wagner, 2008). It means an individual is interested in controlling and influencing the data about themselves. Information privacy also means collecting information, processing information, dissemination of information, and its invasion. Control of one's personal information over secondary usage is one definition of information privacy. The process of employing data for reasons other than those for which they were originally acquired is known as a secondary usage. As a result, information privacy covers gathering, improper access, secondary use, and errors.

The term "Internet privacy" has been used when talks on privacy and concerns related to it arise. It means information about an individual and when it goes on the internet and their concerns regarding regulatory measures and profiling (Cranor L.F.1999).

In this digitised age, communications are digital, and information is stored everywhere, thus creating information privacy. In e-commerce transactions, the trust is not only between consumers and the e-commerce platform but also the internet involves trust between the consumers and the computer system where transactions take place (Clarke, L, Miller& Wiley, 2002).

One of the major concerns on privacy that the researcher will analyse in this paper is related to e-commerce and the violation of one's privacy while using e-commerce platforms via the internet. The question is, why do individuals react to information privacy?

***1.5.2.1 Gaining Monetary benefits by violating privacy***

Another concern is monetary incentives and the monetization of data by e-commerce companies. Companies use various technologies like to name a few, privacy-invasive technologies (PITs) to infringe on consumers' information privacy. In e-commerce, consumers want their information to be used lawfully and for legitimate purposes (TSAI, 2011). However, companies monetise the information received to make additional revenue and money from the information received from the consumers. This leads to conflict and how to balance privacy practices and companies' approaches. If companies push the envelope too far to generate only profits, there is a considerable risk of alienating their consumer base. Companies gain a competitive advantage by using consumers' information and converting it into valuable data.

Often, individuals are not informed about the privacy practices and how their information is divulged, and the practices they should adopt (Meinert, D. B., Peterson, D. K., Criswell, J. R.& Crossland, M. D. 2006). E-commerce companies do not provide proper privacy policies, protection policies, etc. The e-commerce companies do not have such rules, or they do not implement them effectively if they have. In the USA, companies have a privacy policy, but why they do not comply with the guidelines is the concern. Fair Information practices should be included in the privacy policies. There should be technologies and tools that enhance privacy in the digital world. Tools should be designed to reduce the risks involved in online transactions on e-commerce platforms. There are different privacy policies of companies and different attitudes regarding privacy between the companies. According to some research, it is shown that corporations in the U.S.A. have other privacy concerns than Canadian corporations. It is

necessary to explore the differences between privacy policies and their effects on consumers and individuals. Individuals should read and understand privacy policies to protect their interests. More and more information privacy studies should be undertaken at different levels, including individuals, organisations, groups, etc. Privacy is thus infringed by tracking and collecting data, choices, preferences, and data sharing with third parties.

The Federal Trade Commission describes privacy as a choice, access, notice, and security as part of privacy policies (Miyazaki, A.D., Fernandez, A., 2001). Security means protection against destruction of data, disclosure of data, alteration of data, etc., through unauthorised access, attack on data transactions, etc.

It is not correct to violate human rights, and being e-commerce of goods; they have no right to gather the personal information of consumers and sell it to third parties. The question of serving customers in a better way is questionable when privacy is infringed.

***1.5.2.2 Breach of trust by e-commerce companies***

There are many scholars and researchers who believe that e-commerce has created security and trust issues. The first and the most crucial step is to ensure consumers that their personal information will be protected and safeguarded. Consumers are the king of the market. If they do not believe in web merchants, then it will not be possible for e-commerce to survive in the market in the longer run. Once security apprehensions have been talked about, consumers will contemplate the features of the web to know the extent of trust with the e-commerce entities. Trust is one of the essential features for the growth of e-commerce platforms, and privacy concerns of consumers impact the consumer internet market. Many consumers do not reveal their personal information like credit card numbers to e-commerce companies. This also affects other party-related transactions and lack of trust (Cheung, C.M.K., Lee, M.K.O., 2001). To combat this, security and privacy issues must be addressed by including authenticated privacy and security policies on the websites of e-commerce companies. Security and privacy policies of e-commerce companies must be understandable, and encryption and password protection should be enhanced more.

There are various groups, to name a few, TRUSTe or BBBOnLine, that help business organisations to give better protection and security to their consumers. For example, TRUSTe states to consumers, “When you see the TRUSTe seal, you can be assured that you have full control over the uses of your personal information to protect your privacy.” (Garbarino, E., Johnson, M., 1999). The company can display the third-party privacy "seal" confirming their participation once they've joined the programme. Companies are increasingly communicating their commitment to security by using third-party security seals (e.g., Verisign). This will make the consumers secure and trust the e-commerce website to provide their personal information. Privacy statements make consumers feel that e-commerce entities will not share their data with third parties or other organisations (David Gefen, 2003). An IBM Multi-National Consumer Privacy Survey conducted in 1999 found that respondents in the USA believed they had lost control over their personal information. Some respondents chose not to utilise e-commerce platforms to purchase goods because doing so would result in the collection of their personal data (David Gefen, 2000).

Privacy issues in e-commerce markets have become more complicated in recent times because of the growth and development of the internet and technology. A New York Times report revealed in a survey that privacy concern is the main reason behind less development of e-commerce. Ninety-two per cent of the internet users do not shop online and do not trust online websites and companies regarding their personal information (José María Cavanillas, 2016). A project by the World Wide Web was launched, i.e., Platform for Privacy Preferences which helped the users to gain more control over their information.

The Internet of Things has led Indian consumers to visit various websites. The websites track the clickstream data and use their data as inventory to fulfil their interests. They tailor the information like preferences, choices, likings, etc., and then use it for innovative products and advertising. Clickstream data is collected through cookies, spyware, etc. These techniques and tools help in processing data outside Indian territory unprecedently. This is also called behavioural marketing, and it is necessary to protect data collected through behavioural marketing. Cookies are useful because they can be used by a website to track a consumer's computer, for example, shopping cart, login name, surfing activities, etc. It helps to know when the website is visited, the duration of the visit, preferences, etc. are stored on the computer and tracked.

The Internet of things tracks the movements of consumers and collects data to make decisions, and consumers do not have any idea about their invasion of privacy by these marketers like e-commerce. On e-commerce platforms like Amazon, Flipkart, Myntra, etc, the consumers have products in their cart that they purchase or wishlist for future purchases. By using credit cards, etc, the customers compromise their privacy in return for something of value like discounts, coupons, free delivery of products, etc.

### 1.5.3 Technological development and privacy concerns

The technologies used today are destroying privacy at a very fast pace. These privacy-destroying technologies are divided into two categories i.e., to acquire raw data and secondly to process and collate raw data into many streams (Richard O. Mason, 1986). When data accumulation happens, it enables the marketers like e-commerce companies to construct the profiles of individuals for marketing, monetisation, etc. Acxiom is a single firm but it has collected data about the personal and financial information of almost every citizen of the US, UK, and Australia. Data has commercial value and therefore banks also collect information about their customers (Anirudh Burman, 2020).

In online shopping, trust is needed more than in offline shopping. According to Behavioural economics trust and faith are the important triggers for buyer-seller to fulfil the trade relationships.

Businesses have a social responsibility as they cannot operate in a vacuum and it has far-reaching effects on society. Decisions are based on a cost-benefit analysis to maximize profits. The theory of *moral minimum* i.e., that businesses and corporations should not make a profit in such a manner that they harm others. Businesses should avoid or correct the injury caused because of their activities in order to perform the duty of social responsibility (Jose, Edward Curry, Wolfgang Wahlster, 2016).

Another important theory of corporate citizenship is of the view that the businesses are bestowed with the responsibility of doing well and solving the social problems, for example, corporate social responsibility, education, hospitals, etc.

Consumers have accepted e-commerce and theories like TRA (Theory of reasoned action) applicable to the technology-driven environment along with TAM (Technology acceptance model) because e-commerce usefulness and ease of use are the key drivers of the wide acceptance of e-commerce and reliability on the merchants. Trust is another factor that plays an important role in acting as a catalyst to provide consumers with satisfaction with the e-commerce transactions and economic exchange too. (Glen H. Elder, Eliza K. Pavalko, Elizabeth Clipp ,1993). If we analyse the consumer-retailer exchange relationship then also the very first step is an exchange of data between the two such as browsing, gathering information, etc. The second step is whereby the consumer provides personal information by registering email, names, address, preferences, applying filters, etc. The information is captured because of cookies, log- data as well as data -mining tools (Marl Linscott, Anand Raguraman, 2020) The last step is all about the invasion of privacy and monetary information of consumers such as debit/ credit card information, etc. The author Palmer argued that for e-commerce business activities trust is the most important factor.

The e-commerce and the growth of the internet have actually led to a revolution in the manner of conducting e-commerce operations and businesses. The business is conducted electronically through domain names. Many businesses do not have a physical location but are conducting businesses online etc.

### 1.6 Need for specific legislation in India

The protection of data and privacy can be achieved through stringent laws, and policies of data governance, so that there is at least less intrusion into privacy. There is no particular legislation in India pertaining to personal data protection and preventing infringement of privacy. Current legislations delating with this issue are “The Information Technology Act, 2000”, Indian Penal Code 1860, The Constitution of India, The Indian Contract Act, 1872, Intellectual Property Rights, and the draft “Data Protection Bill, 2021”. The Data Protection Bill, 2021 was earlier named “The Personal Data Protection Bill, 2019”. The Information Technology Act, of 2000 addresses the issue of identity theft, malicious attacks, computer attacks, data stealing, etc but does not address the current issue of infringement of privacy and data protection of individuals. The Act imposes civil liability and criminal liability for the disclosure of personal information if the consent of the data subject is not taken. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have taken the place of the Information Technology (Intermediary Guidelines) Rules, 2011 and due diligence is to be followed by the intermediaries, grievance redressal mechanism, code of ethics, self-regulatory bodies, etc. But there is no specific rule or guideline regarding e-commerce using data collected and stored for the purposes of monetisation.

However, “Consumer Protection (E-Commerce) Rules, 2020” apply to e-commerce business models, e-commerce retails, goods and services sold or purchased on digital networks. The duties of e-commerce entities are prescribed by the rules regarding non-adoption of unfair

practices, and liabilities on marketplace e-commerce entities are also imposed. Nothing related to the practices of data monetisation is governed by these rules and regarding the protection of privacy of the consumers.

The Right to Privacy was deemed a Fundamental Right in India by the Supreme Court in Justice K.S. Puttaswamy (Retd) and Another v. Union of India. After that, a Justice B.N. Srikrishna-led expert group drafted the Personal Data Protection Bill, 2019 with the intention of safeguarding sensitive information and avoiding data leaks. Because it is impossible to distinguish between personal and non-personal data, the Personal Data Protection Bill, 2019, was renamed to the Data Protection Bill, 2021 on December 16, 2021. It stipulates that the Bill must be implemented within 24 months to provide data processors and data fiduciaries time to make the required adjustments to their procedures and policies.

This Bill is applicable to the personal and non-personal data of a natural person. The Personal Data Protection Bill, 2019 provides for the protection of the privacy of the individuals in relation to the personal data. The processing of personal data and protection of the rights of the individuals in this process is very important to create a trust relationship between the persons and entities processing the personal data. The Bill also provides for the establishment of a Data Protection Authority.

The key players are-

1. Data Principal
2. Data Fiduciary
3. Data Auditor
4. Data processor
5. Data Protection Authority

Data fiduciaries are created in the Bill to determine the purpose of processing personal data of the subjects called data principals. Various obligations are imposed upon the data fiduciary for example, giving notice to the data principal for the collection of data, the purpose and nature of the processing, and grievance redressal mechanism is also provided in the bill for better redressal of grievance of the consumers. The personal data can be processed only for specific, clear and lawful purposes by the data fiduciary. Chapter II of the Bill provides the obligations of the data fiduciary and the legal obligations while processing the personal data. The processing of data can be done only in a fair and reasonable manner and the purpose for which the data principal has consented or any purpose related to it the processing of personal data will be collected. Section 17 of the Bill provides that the data principal shall have the right to confirm from the data fiduciary whether the data has been processed or not processed, the right to access the identity of the data fiduciary with whom the personal data has been shared with. Section 18 of the Bill gives the data principal a right to the correction of personal data or to update personal data. Section 19 of the Bill provides the right to data portability to the data principal and right to be forgotten under Section 20.

The Bureau of Indian Standards in mid-June introduced standards for data privacy the IS 17428. It is a framework for the organisation to improve the data privacy management system.

It assures the customers and the employees about the privacy practices adopted by them and provides quality assurance of goods in the country.

The "European Union's General Data Protection Regulation, 2018" is the strictest law in the present times. It has given the ownership of data to its citizens and also requires permission to use data commercially.

**1.7 Conclusion and Policy Recommendation**

Privacy is the absolute prerequisite and not something that one is entitled to. Every day we generate a huge amount of personal data without caring about our own privacy and protection. For example, we wear smart wrist watches embedded with various applications, and before our alarm rings on our mobile phones, etc, one's heartbeats, blood pressure, and sleeping patterns are recorded. We use Spotify, Apple or Google news, Quora, WhatsApp, Uber, Ola, etc for interests and entertainment but the cost that we are paying is invisible and i.e., constant surveillance of our choices, day-to-day activities and actions, are being recorded enormously by the technology-driven devices. There are so many online dating and relationships apps like OK Cupid, match.com, etc, whereby personal profiles are created by the users revealing their names, gender, age, sexual orientation, etc, making these online apps a global industry generating billions of dollars.

In 2016, the data of 70,000 users on Ok Cupid app was published by Danish researchers by violating the terms of use of Ok Cupid. Their justification was that the information was not private meanwhile raising several questions pertaining to legal and ethics. For example, did the researchers had obligation to take the consent of Ok Cupid members for the use of their personal information? What would be the monetary damages given to the users, etc?

E-commerce companies are playing a very significant role in the times of the digital world where everything is connected with the internet of things. E-commerce is a growing area, and with technological advancements and artificial intelligence, they are offering better and more advanced services and products to consumers in an easy manner. At the same time, legal issues are also involved with the growth of e-commerce companies because these companies are no doubt providing their best but also infringing the privacy of consumers instead of providing better services. They collect and store their data which is later analysed by the various techniques used by the e-commerce companies to make use of the raw data for their monetisation purposes to generate revenue at the cost of the consumers' trust. The trust paradigm is based more on fiduciary law, and if trust is broken, then the e-commerce companies will also fail in the coming times. Trust plays a very significant role in the growth of e-commerce companies.

There are various guidelines like The OECD 1999 guidelines that provide that consumer should have access to e-commerce. There should be confidence and trust of consumers in e-commerce to check and control unfair, misleading practices. There should be an effective redressal system. Due to advancements in technologies, the OECD 2016 revised the recommendations of 1999 to address the issues and menace of e-consumers protection to address and report the problems of data privacy and security of e-consumers.

In India, there is a lack of comprehensive policies and laws on data protection and the privacy of individuals is a matter of concern in the era of globalisation. The policies of e-commerce should be in line with notice-and-choice so that the consumers know how their data will be used if they have consented to provide their data to them. In the United States of America, the California Online Privacy Protection Act, 2020 requires that commercial websites will provide users with privacy disclosures. In 2003 California introduced the "Shine the Light" law to allow the residents of the state to know if their personal information has been shared by the companies with the third parties.

India has undoubtedly drafted the Data Protection Bill, 2021, along with the European Union's General Data Protection Regulation, 2018. Still, it has to be seen how far they are suitable for the Indian conditions and e-commerce players in the Indian market. Once enacted, the bill will provide for Data Protection Officers, data processors, and data controllers. Their roles and responsibilities are well explained in the bill so that no scope of lacunas is left behind. There is a rigorous need for legal mechanisms to govern the challenge being faced by sharing our personal information. Code of conduct by e-commerce companies in the collection of data, processing of data, or transferring data to any other country should be observed so as to give protection and shield to the right to privacy of the individuals.

**References**

IBEF. (2022*). E-commerce Industry report [Online],* Available at: https://www.ibef.org/industry/ecommerce. Accessed April 24, 2022.

Cranor, L.F. (2017). Internet privacy. *Communications of the ACM,42(2), 28*

Edward J. Walters. (2021). Data-Driven Law: Data Analytics and the New Legal Services. [Online] Available at: https://www.taylorfrancis.com/books/edit/10.1201/b19763/data-driven-law-ed-walters. [Accessed 2022]

Viktor Mayer-Schonberger, Kenneth Cukier. (2013). *Big Data A Revolution That Will Transform How We Live, Work, and Think.* [Online] Available at: https://www.amazon.in/Big-Data-Revolution-Transform-Think/dp/1848547927. [Accessed 2022]

Marl Linscott, Anand Raguraman.(2020). *Aligning India's Data Governance Frameworks.* [Online]. Available at: https://www.jstor.org/stable/resrep25999. [ Accessed June 2022].

Anirudh Burman. (2020). *Conclusion: A more Pragmatic, Privacy- oriented approach to Data Protection*. [Online]. Available at: https://www.jstor.org/stable/resrep24293.8.[ Accessed 2022].

Tara J Radin. (2001). *The Privacy Paradox: E-Commerce and Personal Information on The Internet.* [Online] Available at: https://www.Jstor.Org/Stable/27801264. [Accessed 2022].

Glen H. Elder, Eliza K. Pavalko, Elizabeth Clipp. (1993). *Working with archival data: Studying Lives*. [Online]. Available at: https://methods.sagepub.com .[Accessed 2022].

Janice Y. Tsai, Serge Egelman, Lorrie Cranor and Alessandro Acquisti. (2011). *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.* [Online] Available at: https://www.jstor.org/stable/23015560. [Accessed June 25, 2022]

Maureen K. Ohlhausen Alexander P. Okuliar. (2015). *Competition, Consumer Protection, And the Right Approach to Privacy.* [Online] Available at: https://www.ftc.gov/system/files/documents/public_statements/686541/ohlhausenokuliaralj.pdf. [Accessed 24 May 2022].

France Bélanger & Robert E Crossler. (2011). *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.* [Online] Available at: https://www.jstor.org/stable/41409971. [Accessed 2022]

McKinsey& Company. (2017). *Monetising Data: A New Source of Value in Payments.*

Phillip Russom. (2011). *Big Data Analytics*. TDWI Best Practises Report.

José María Cavanillas, Edward Curry, Wolfgang Wahlster.(2016). New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe. [Online] Available at: https://link.springer.com/book/10.1007/978-3-319-21569-3. [Accessed on May 2022]

Abou Zakaria Faroukhi, Imane El Alaoui, Youssef Gahi and Aouatif Amine. (2020). *Big data monetization throughout Big Data Value Chain: a comprehensive review.* Available at: https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-019-0281-5.pdf. [Accessed 2022].

Richard O. Mason. (1986). *Four Ethical Issues of the Information Age*. Available at: https://www.jstor.org/stable/248873?origin=crossref. [Accessed 2022].

Joseph Phelps, Glen Nowak and Elizabeth Ferrell. (2000) *Privacy Concerns and Consumer Willingness to Provide Personal Information.* Available at: https://www.jstor.org/stable/30000485. [Accessed 2022]

Anthony D. Miyazaki and Ana Fernandez. (2001). Consumer perceptions of privacy and security risks for online shopping. Available at: https://www.jstor.org/stable/23860070.[ Accessed 2022].

Christy MK Cheung, Matthew.K.O. Lee. (2001). *Trust In Internet Shopping: Instrument Development and Validation Through Classical and Modern Approaches.* Available

at:https://www.researchgate.net/publication/220500356_Trust_in_Internet_Shopping_Instrument_Development_and_Validation_through_Classical_and_Modern_Approaches. [Accessed 2022].

Ellen Garbarino and Mark S. Johnson. (1999). *The Different Roles of Satisfaction, Trust and Commitment in Customer Relations.* Available at: https://www.jstor.org/stable/1251946. [Accessed 2022].

Kiersten E. Todt. (2019). *Data Privacy and Protection: What Businesses should do.* Available at: https://www-jstor org.gnlu.remotlog.com/stable/26843891?searchText=data+protection&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Ddata%2Bprotection%26so%3Drel&ab_segments=0%2FSYC-6451%2Fcontrol&refreqid=fastly-default%3Ad0b4401330e24ddc31d07d054664e37a#metadata_info_tab_contents. [Accessed April 2022].

Dhiraj R. Duraiswami, (2017). *Privacy and Data Protection in India*. Available at https://www.jstor.org/stable/26441284 .[ Accessed June, 30, 2022].

Anneliese Roos. (2006). *Core Principles of data protection law*. [online] Available at: https://www.jstor.org/stable/23253014. [Accessed 2022].

Mira Burri, Rahel Schar. (2016). *The reform of the EU Data protection Framework: Outlining Key changes and assessing their fitness for a Data- Driven Economy.* [Online]. Available at: https://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479.[Accessed May, 28, 2022].

Nicholas D. Wells, Poorvi Chothani, James M. Thurman. (2010). *Information Services, Technology, and Data Protection.* [Online]. Available at: https://www.jstor.org/stable/40708252. [Accessed 2022].

Shiv Shankar Singh. (2011). *Privacy and data protection in India: A critical Assessment*. [Online]. Available at: https://www.jstor.org/stable/45148583. [Accessed May, 2022].

Will Thomas, De Vries.(2003). Protecting Privacy in the Digital Age. [Online]. Available at: https://www.jstor.org/stable/24120519. [Accessed May, 2022].