ISSN: 0974-5823 Vol. 7 (Special Issue, Jan.-Feb. 2022)

International Journal of Mechanical Engineering

Protecting The Privacy of Digital Consumers in An Artificial Intelligence-Driven World

Aditya Agrawal[1] Tulika Singh[2] Upasana Khattri[3] Paridhi Sharma[4]

[1,2,3,4,]Academic Tutor and TRIP Fellow, Jindal Global Law School

Abstract. Consumer attractiveness and loyalty are at the heart of every organization, particularly in this information age, where digital consumers are on the rise. Online businesses have begun to use Artificial Intelligence (hence referred to as AI) to better understand their customers and give them the best possible experiences on their platforms to sustain their customer base. Consumers' demands are met by AI, which records their preferences and automatically presents them with options depending on their interests. As a result, customers are more likely to interact with businesses because their specific needs are considered. Businesses use AI to collect a lot of personal data from customers by asking them questions about their personal information and documenting their surfing behaviors to keep their customer base. Second, these online business platforms inform, promote, and publicize any event or sale on their separate sites via a series of emails or messages, even if customers do not subscribe to such notifications. Individuals' privacy is invaded by these consumer seduction practices, which expose firms to lawsuits. First, we will explore how businesses have used AI to win customers and how it is affecting the economy in the context of the Indian digital market in this paper. Second, we will examine customer interests and choices, as well as their knowledge of consumer protection and related regulations, through an empirical study. Finally, we will discuss the privacy concerns raised by the use of AI and the concept of digital consumerism.

Keywords- Artificial Intelligence, Privacy, GDPR, Consumer Protection

WHAT IS ARTIFICIAL INTELLIGENCE, AND HOW DOES IT WORK?

Artificial Intelligence (hence referred to as AI) has no clear definition, however, it is defined as machines capable of doing activities that need human intelligence.[1] They gain knowledge from their experiences, enhance their abilities, and answer cognitive questions. They can mimic certain aspects of the human mind, such as learning, problem-solving, and language interactions.[2] AI was created to assist humans in completing complex activities and making complex decisions. It also reduces the amount of hard human labor required, making our lives more comfortable and convenient. AI works by combining massive amounts of data with clever algorithms to assist software in learning from patterns. It compiles data from several sources, analyses it, and generates an explanation. Machine learning, deep learning, neural networks, cloud computing, natural language processing, and computer vision are all important components of AI. Narrow AI and Artificial General Intelligence are the two broad kinds of artificial intelligence. Narrow AI entails effectively completing a particular task, but it does so under constraints and limitations, and it lacks even fundamental human intelligence, such as weather prediction. Artificial General Intelligence, often known as strong AI, is a type of AI that has general intelligence similar to humans and uses that intelligence to complete tasks, such as Advanced Robotics. AI has progressed substantially over the years, and it is predicted to reach 99.94 billion dollars by 2023, growing at a compound annual growth rate of 34.86 percent.[3] The AI market in India was valued at 6.4 billion dollars in July 2020, and it is likely to increase in the next years, contributing significantly to the country's GDPR.[4] AI is being used in a variety of fields, including health care, business, and government, to assist in job completion and reduce the load of human labor. E-commerce Virtual assistant AI technology, such as Amazon Echo, Google Assistant, and Siri, has also been developed by businesses to assist consumers with daily tasks.[5] Consumers can use their voices to command these virtual assistants to accomplish various tasks. Play music, obtain information, remind them of pending duties, operate their smart homes, read the news to them, and so on. Wearable devices such as fit bits and smartwatches also employ AI, which people use as healthcare tools since it allows them to check their heartbeats, record their sleep durations, and provide healthcare advice, but it also has other uses. AI is dynamic because it can do a range of activities; as a result, it has been welcomed all over the world, and its performance is projected to become more diverse and accurate in the future. Businesses all over the world have substantially adopted the use of AI. The major goal is to improve customer experiences and keep their customer base. Business companies use Artificial Intelligence to give excellent experiences to their customers while also collecting customer data through personal queries or recording browsing behaviors to entice customers.[6]

AGGREGATORS AND THEIR INFLUENCE ON CONSUMER PURCHASE INTENT

Producers, distributors, and consumers make up the majority of the market's distribution route. The role aggregators6 is an addition to the indirect distribution channel under the indirect distribution channel. Aggregators are large internet business platforms that bring together several service providers under one brand name.[7] Websites or mobile applications are used to create these platforms. For example, platforms like Amazon, Uber, Swingy, and others combine products from a variety of service providers, such as local vendors, and communicate directly with their customers under their brand names only.[7] These aggregators specialize in intent-based marketing, which entails promoting a product or service based on an individual consumer's desire and intent to buy, as

evidenced by their purchasing behavior and browsing habits.[8] It also looks at external data to see what its customers are looking for on different platforms or websites. Such businesses acquire a large amount of consumer data not just from their platforms, but also from the user's general actions on similar platforms.[8] They then turn these data into valuable commodities, which they employ to cater to their customers' specific demands. For example, Netflix recommends videos based on previous viewing behavior. Amazon, too, makes product recommendations based on prior purchases or most browsing patterns. They've also devised techniques such as dispatching the order. They send out the order even before the customer places it. Amazon uses this strategy for Amazon Fresh and Amazon Prime Products, in which it forecasts product demand using Artificial Intelligence based on purchase intent and interest of consumers in a specific area; based on this information, groceries or prime products are already stored in that area's warehouse, and customers receive them within a few hours of placing an order.[9]

Amazon can attract significantly more customers and expand its customer base than its competitors with such a speedy delivery method in place and the added benefits of Amazon Prime Subscription. This is an example of how aggregators like Amazon use artificial intelligence to collect personal information from their customers and turn it into precise commodities for profit.

The concept of entity resolution and how it might be used to sway customers.

People engage in different activities in their daily lives as consumers, such as surfing across multiple social media platforms, making online purchases, and so on. Through these actions, they reveal their credit/debit card information, location, and hobbies. With the help of Artificial Intelligence, this information is stored as consumer data points, which are then used by businesses as touchpoints to target consumers by providing personalized products based on their interests and promoting products that they are likely to buy, allowing consumers to choose their brand over their competitors.[10] Because so much data is created every day, programmes like Google Analytics integration and store all of a consumer's data points using an analytical model called Entity Resolution13, which uses data from other external data collection businesses.

This strategy is used to understand each customer's unique preferences and interests, allowing businesses to sell them products that they want, promote relevant advertising, and run political campaigns, among other things.[11] In the infamous Cambridge Analytica case, for example, Cambridge Analytica, a political consulting business involved in Donald Trump's 2016 presidential campaign in the United States of America, got personal data from about 87 million Facebook users' profiles with the help of Facebook.[12] Facebook admitted to leaking 87 million users' personal information to Cambridge Analytica, which was then utilized in Donald Trump's campaign.[12] These users' information was gathered through a Facebook personality exam in which users' hobbies, location, favorited pages, preferences, purchase intent, and other factors were logged to determine their political leanings. Potential voters were controlled and swayed with the use of this to get the greatest number of votes in their favor. The concern here isn't so much how Cambridge Analytica aided the campaign as it is how a massive platform like Facebook released millions of users' data without their knowledge. Facebook users give away a lot of data in their daily lives. All of their data is retained by Facebook, which keeps track of their activity, from uploading photos to revealing their location, the places they frequent, and their individual choices, among other things. Second, it has the option of deactivating an account rather than permanently deleting it, implying that even after a user deactivates his or her account, his or her data or previous activities will be stored indefinitely, implying that even if users want to delete all of their data, they do not do so. Finally, Facebook allows users to connect to third-party apps, allowing it to track their actions on other platforms. As a result, Facebook stores more data than is shared on its platform. All of this information is gathered using artificial intelligence (AI) through quizzes, games, and favorited pages, among other methods.

In India's digital market, the situation is as follows: According to projections, the Indian e-commerce sector is predicted to grow at a quicker rate, reaching 200 billion dollars by 2026[13] and 850 million users by 2025.[14] It is also expected to surpass the United States of America to become the world's second-largest e-commerce market by 2034.[15] The extensive online campaign and marketing that these business giants have undertaken, which has established a new arena for customer expectations,[13] can be traced to this paradigm shift from physical shopping to online consumerism. Consumers find shopping on online platforms to be simple and timesaving, as well as providing them with speedier and less expensive services. Furthermore, huge online discounts such as Flipkart's Big Billion Sale, Amazon's Great Indian Festivals, and others allow consumers to buy a good quality product at a lower price, which encourages them to use these platforms more. Then there were features like voice search and search in local languages via images, which drew the attention of Indian customers and made it easier for them to shop online. Loyalty programmes, such as subscription services, have also aided this e-commerce in building their loyalty base by delivering tailored services that make customers feel special, as well as keeping customers close to their websites. All of this indicates how these companies entered the Indian industry and established a more secure position in the digital market. They have used AI technology to gain a better understanding of the Indian mindset, and as a result, they have developed strategies that are tailored to the Indian market. As a result, it is possible to break into the Indian market. Consumers are so enamored with platforms that they freely give away their personal information to these corporations, who then turn it into valuable commodities for their operations.

Consumers' Digital Challenges

Online platforms, often known as E-commerce, are incredibly powerful and have a significant impact on consumer behavior. They collect so much information on their customers, in the form of cookies and other means, that it's easy for them to manipulate them into buying items or using services that they wouldn't have done otherwise. These websites use deceptive messaging to sway their customers' interests, such as claiming that a specific product is doing well and that if they do not purchase it, they would lose it to

other customers. These messages encourage customers to make an impulse buy, even if they have no intention of doing so. They employ tactics such as making the availing of service button stand out in bright colors to draw the customer's attention and burying the opt-out of service link in a drop-down menu or anywhere else that is difficult to see. Second, consumers find it difficult to entirely forsake widely utilized digital platforms such as Facebook, which has purchased other social media platforms such as Instagram, WhatsApp, and others. Furthermore, in the absence of a safer alternative, consumers are concerned that if they exit the platform, they will lose all of their connections built through it.[16] Many users also find it easier to log in to third-party apps using their Facebook account rather than creating a new account every time they visit a new website. Platforms such as Amazon devise strategies to retain and attract customers by offering a variety of incentives such as faster delivery, discounts, and personalized products, among other things, which earns the customers' trust and makes it difficult for them to switch without putting in a lot of effort.[16] As can be seen from the preceding discussion, large online platforms have established themselves throughout the digital market, and in the absence of any other safer options, consumers are forced to use them. Furthermore, with the emergence of the Internet of Things, businesses can follow their customers' every step, making it very easy for them to manipulate their customers' purchase decisions and generate interest in specific products or services. Consumers are being regulated to such an extent by online platforms that it is becoming difficult for them to make informed decisions in the digital market. This demonstrates the online platforms' power and control over consumers, resulting in an uneven ecology for consumers. In India, several laws are relevant to consumers.

The General Data Protection Regulation (GDPR)

GDPR is the cornerstone of Europe's digital privacy legislation, as well as the most comprehensive data protection and privacy regulation ever enacted. It establishes specific guidelines for the creation, movement, administration, and storage of personal data.[17] The primary goal of this regulation is to simplify the regulatory environment so that citizens and enterprises in the European Union can reap the full benefits of the digital economy. It was designed and passed by the European Union (EU) and went into effect on May 25, 2018, overriding the Data Protection Directive (DPD). It imposes hefty fines on anyone who violates its security and privacy rules, with penalties ranging from tens of millions of euros.

In our day-to-day lives, data is extremely crucial. Every service we use, from social media to businesses to banks and governments, analyses and collects our data. Organizations compose and, maybe most importantly, save our names, addresses, credit card numbers, and much more. Organizations must ensure that personal data is collected legally and under stringent conditions, and individuals who gather and manage it must protect it from exploitation and misuse, as well as respect the rights of data owners, according to the GDPR rule. The regulation relates to two separate sorts of data handlers[18]

Processors\s-Controllers

A controller is a person or a public authority who collects personal data alone or in collaboration with others and also explains what will happen with the data, whereas a processor is a person or a public authority who processes personal data on behalf of the controller. To put the data protection principles into practice, controllers and processors must take appropriate practical and administrative steps. They should keep privacy in mind when constructing the information system. The data processing shall be done on one of the six legal bases listed in the rule, which are: (Consent, public task, contract, vital interests, legitimate interest, or legal requirement). When the processing is based on the data subject's consent, the data subject has the right to withdraw consent at any time.[19]

WHAT TYPES OF DATA ARE AFFECTED BY THE GDPR?

The GDPR is primarily concerned with personal data. Personal data refers to any information about a data subject or consumer that can be used to identify them directly or indirectly. A name, an e-mail address, a photo, biometric data, or a person's computer's IP address are all examples of personal data. The question of whether or not an IP address is deemed personal data under GDPR has been debated. The senators subsequently clarified that IP addresses will be considered personal data because a person's identity can be linked back to his IP address.[19] Data with clear personal identifiers like first and last names may be subject to the GDPR depending on how difficult it is to deduce an individual's identity from that data.

PERSONAL INFORMATION THAT IS CONFIDENTIAL

The GDPR prohibits the processing of personal data that reveals a person's racial or ethnic origin, political, religious, or philosophical beliefs, or trade union membership, as well as the processing of genetic and biometric data to identify a natural person, and data about a person's health, sex life, or sexual orientation. If the individual has specifically granted his or her approval for the processing of their data, or under a few other specified conditions, the above-mentioned statement will not apply.

DATA RELATING TO CRIMINAL ACTIVITIES

Processing of data relating to criminal convictions and offenses, or security measures, is only permitted under the GDPR when it is carried out under the supervision and control of official authority, or when the processing activity is authorized by Union or Member State Laws that provide appropriate safeguards for the data subjects' rights and freedoms. Under the supervision and control of the official authorities, a comprehensive record of criminal convictions must be kept. There should be a valid basis for processing

personal information about criminal offenses or convictions under Article 6 and an official authority for processing under Article 10.[20]

CHILDREN'S INFORMATION

The GDPR includes rules aimed at improving the protection of children's data and ensuring that children are addressed clearly and understandably. Transparency and responsibility are critical when it comes to protecting the data of children, especially when they use internet services.

WHO ARE THE PERSONS AFFECTED?

This legislation applies to firms operating within the EU as well as organizations operating outside the EU that provide goods and services to EU customers or businesses. As a result, practically every large company in the world requires a GDPR compliance strategy. Now that businesses are amassing more personal data, this new regulation is intended to provide individuals with better control over their data.

BASES FOR DATA COLLECTION THAT ARE COMPLYING WITH THE LAW

These four lawful bases were adapted from the 1998 Data Protection Act's 'conditions for processing,' and under the GDPR, we can only process data if we can demonstrate at least one of the six lawful bases, which include:

1. Consent: Consent is the most solid of all the legal bases since it addresses GDPR's core goal, which is to give individuals complete control over their data. In essence, the subject must give explicit permission for their data to be processed for a specific reason.

2. Contract: Data processing is required to conclude a contract with the data subject. If the processing activity is not comparable to the contract's provisions, the data processing activity must be covered on a separate legal basis. When it comes to processing payment information, this will be the starting point.

3. Legal Obligation: There is a legal obligation for the processing activity, such as employment, information security, or consumer transaction statute. For example, to comply with a court order, an individual may be required to process his or her data. It's a good idea to mention what statutes or authorities a person can report to when quoting their legal obligation.

4. Public duty: This refers to gathering information in the public interest, such as completing a duty assigned by a government agency. It usually does not apply to private organizations, but it also does not necessitate statutory authority for data processing. Individuals cannot assert this reason if they can avoid data processing.

5. Legitimate Interests: The processing activity is necessary for our or a third party's legitimate interests unless there is a compelling cause to protect the person's personal information that outweighs those legitimate interests. This foundation will not apply to a government agency that uses data to carry out its functions.

6. Vital Interests: This foundation refers to necessary processing, but also to situations in which permission is not required. According to this reading of the basis, a person can respond on this basis if they need to protect someone's life, but they can't gain consent for the processing activity otherwise.

GDPR COMPLIANCE[21]

It refers to the act of ensuring that corporate activities and operations are compliant with the GDPR's laws.

TERMS AND CONDITIONS OF THE GDPR

Under GDPR, there are six key principles to follow. Article 5 of the GDPR contains these principles for the processing of personal data. Personal data must be based on the following criteria, according to this article:

Lawfulness, Fairness, and Transparency are the guiding principles.

Special focus is placed on personal data being managed in a way that offers a clear explanation for people whose information is being created and managed under this 6principle. This is the principle;[22]

a) To process data, an organization must establish a legal justification for collecting it.
b) Concerning data subjects, data should be administered legitimately, fairly, and transparently.
c) Data should only be collected for specific and legitimate purposes, not for any other reason.

Concept of Purpose Limitation

this principle requires that an organization have a policy on the collecting of personal data, that the personal data is used for a specific purpose with the data subject's prior consent, and that the personal data is not misused or exploited.

Data reduction principle

Many firms collect and keep significant volumes of data for a variety of reasons, including marketing, research, and monitoring. Regardless of the size of an organization or the type of data it stores, it is recommended that the organization analyze the value of the information stored and that any data held be limited to only that which is necessary by the organization for defined purposes.

Principle of truth and accuracy

To ensure GDPR compliance with this principle, enterprises must have a comprehensive policy and procedure in place for regular reviews. All businesses will be forced to have an up-to-date database of their customers and staff.

Integrity and confidentiality principle

This concept covers all aspects of security. It is the organization's responsibility to ensure that all required safeguards are in place to protect the personal information held by their data subjects. Such as unauthorized access, unintended harm, and external threats like malware, phishing, or theft. Individuals could be enslaved by weak security mechanisms, causing them distress. The GDPR requires that enterprises have appropriate levels of security to mitigate the risks posed by their processing under this principle.

Storage limitation principle

According to this principle, an organization cannot collect unneeded data that is unrelated to the collection's goal. As a result, before collecting any data, businesses must first determine exactly what they require. Periodic evaluations should also be conducted so that unneeded data can be eliminated after a specific amount of time has passed.

PERSONAL RIGHTS UNDER THE GDPR

Individuals are granted the following seven rights under the GDPR:[23]

1. The right to be informed

- Individuals should be fully informed about how their data is collected and used. The GDPR requires this level of transparency.
- •Individuals have the right to know why their data is being collected and with whom it will be shared.
- Individuals should be informed about their privacy rights when their data is collected.
- Individuals must be given privacy information within one month if personal data is collected from any other source.
- If a person already possesses all of the relevant information, there is no need to present them with privacy information.
- Individuals should be given accurate, transparent, and easily available information.

2. **Access to personal data**[24]

- Individuals have the right to access their data. Subject access is the term for this.
- A request for topic access might be made either verbally or in writing. It takes around a month for an organization to respond to such a request. In most circumstances, there is no price.

3. Right to correction

- Individuals have the right to have their data rectified if it is incomplete. The request for their data to be completed can be made either verbally or in writing.
- The deadline for responding to this request is one month.
- An organization may choose to refuse this request in specific circumstances.

4. The right to be forgotten

- Data subjects can request that their personal information be deleted. 'The right to be forgotten' is another term for this.
- You can make a request either verbally or in writing. The time limit for responding is one month.
- This is not an absolute right, and it can only be exercised in specific situations.

5. The right to data limitation

- Individuals have the right to request that their data be restricted. This is not an absolute right that can only be used in specific circumstances.
- It is possible to make a request either verbally or in writing. The time limit for responding is one month.
- An organization can keep data but not use it when processing is prohibited.

6. Data portability is a legal right.

- Individuals can reuse their data across many services for their purposes.
- They can effortlessly move their personal information from one IT environment to another.
- This enables people to take advantage of applications and services that can leverage their data to get them a better bargain.

7. Right to object

- In some instances, individuals have the right to object to the processing of their data.
- They have a legal right to request that their personal information not be used for direct marketing purposes.
- Individuals must be informed about their right to object.
- You can make a request either verbally or in writing. The time limit for responding is one month.

COUNTRIES WITH DATA PROTECTION LAWS SIMILAR TO THE GDPR

1. California Consumer Privacy Act (CCPA) - United States of America[25]

This rule was passed in 2018 and will go into effect on January 1, 2020. Gives people more rights and protections when it comes to how firms utilize their personal information. It imposes numerous limits on organizations, many of which are comparable to those imposed by the General Data Protection Regulation (GDPR). Customers in California have the following rights:

- •Children under the age of 16 must give explicit approval for their data to be made available for sale.
- Children under the age of 16 must give explicit consent for their data to be made available for sale.
- Ensure that those who exercise their rights under the CCPA are not charged greater rates than those who do not.

2. LEI GERAL DE PROTECAO DE DADOS (LGPD) – BRAZIL

- Also known as the Brazilian General Protection Law, this law was passed by the Brazilian National Congress on August 14, 2018, and will take effect on August 15, 2020.
- Their definition of personal data is very similar to that of the GDPR. The LGPD has indicated in several places that personal data includes any information that can be used to identify a person or subject them to a specific treatment, and it goes farther than GDPR in this regard. Their fundamental rights are also quite similar. Even though the GDPR has eight fundamental rights and the LGPD has nine, they are fundamentally the same rights.

3. THAILAND PERSONAL DATA PROTECTION ACT (PDRA)[26]

- Thailand's National Legislative Assembly approved it in February 2019
- It was published in the Government Gazette on May 27, 2019 and took effect on May 27, 2020. The PDPA and GDPR are similar in the following ways:
- Establishment of a legal basis for the collection and use of personal data • Strict penalties and fines
- Extraterritoriality of application

4. SOUTH KOREA'S PERSONAL INFORMATION PROTECTION ACT

- This rule has been in place since September 2011 and includes several GDPR-like elements. These provisions are as follows:
- Obtaining consent
- Scope of valid data
- Appointment of a Chief Privacy Officer
- Data Retention Period Limitation

INDIA'S DATA PROTECTION LAWS

There is currently no legislation or special law in India that deals with the subject of data protection or the breach of an individual's privacy. Some elements of the Information Technology Act, established by parliament in 2000 and revised in 2008, deal with computer-related offenses or crimes, as well as privacy violations, although these measures are insufficient to address the current situation. The Information Technology Act of 2000 handles concerns such as monetary compensation (civil) and criminal penalties (criminal) in circumstances where personal data is misused or contractual obligations on personal data are violated. India is now debating a comprehensive personal data protection law in a joint parliamentary committee, which includes numerous content-related rules similar to those found in the European Union's General Data Protection Regulation (GDPR).

According to this measure, to collect personal information, businesses classed as data fiduciaries must first obtain consent from the individuals whose data is being discussed. Anybody that determines the purpose and means of processing personal data is considered a data fiduciary. This concept encompasses everything from ride-sharing applications to social media to data brokers who buy and sell customer information.

Extra requirements are imposed by this bill, such as the requirement to seek parental or guardian agreement for the collection of information about children. The bill also contains several exceptions that allow data fiduciaries to harvest personal data without obtaining consent. For example, there are exceptions for state or other entities, law enforcement, and medical situations to comply with court orders. The bill's clauses also provide data principles, or those whose data is being collected, rights. The data principles have the right to inquire about the collection of their personal information from the data fiduciaries. The data principals also have the right to have their data stored by the fiduciary corrected or erased - a "right to be forgotten," as defined by the GDPR. They will also have the right to see their data in a clear and transferable format, with the information organized.

Justice K.S. Puttaswamy vs Union of India and others, 2017 SUPREME COURT JUDGMENT ON THE RIGHT TO PRIVACY

In 2012, retired High Court Judge Justice Puttaswamy filed a writ petition against the Union of India in front of a nine-judge Supreme Court bench, contesting the legitimacy of Aadhar because it violates the right to privacy. He posed the following questions:

1. Is there a basic right to privacy under the Indian Constitution? Is the court's decision in M.O. Sharma & Others vs Satish Chandra, DM, Delhi & Others, and also in Kharak Singh vs The State of U.P., that there are no such fundamental rights, the correct expression of the constitutional position? On August 24, 2017, a nine-judge panel of the Supreme Court of India issued a historic decision affirming the basic right to privacy guaranteed by Article 21 of the Indian Constitution. "No individual shall be deprived of his or her liberty unless following the method prescribed by law," according to Article 21 of the Constitution.

2. The phrase 'privacy' is to be an inherent part of Part III of the Indian Constitution, which lays down citizens' fundamental rights, according to the ruling. The Supreme Court further declared that the state must strike a careful balance between individual privacy

and the legitimate goal, at all costs, because fundamental rights cannot be taken away by legislation, and every law and conduct must be following the Constitution. The right to privacy is not an absolute right, according to the court, and every violation of privacy by state or non-state actors must pass the triple test:

1. Proportionality
2. Legality
3. Appropriate Objective

In providing a legal foundation for the protection of privacy in India, the Supreme Court of India once again appeared as the lone custodian of the Constitution.

CONSUMER PROTECTION ACT 2019

This is the era of commerce and digital marketing, and the number of digital consumers is rapidly increasing. With such rapid expansion, customers confront a plethora of challenges[27]. As a result, to provide a safe environment for digital consumers, the Indian government adopted the Consumer Protection Act, 2019, which, among other things, addresses the concerns that digital customers face. New Act replaces the old Consumer Protection Act of 1986, which mainly addressed offline or marketplace consumer issues; however, this Act also covers and imposes strict liability on online service providers. The Central Consumer Protection Authority, which will be empowered by the Central Government to impose penalties and other reasonableness, has a proper procedure laid down for filing a complaint regarding any dispute and a grievance mechanism set up to address any dispute related to consumer protection. After that, a consumer dispute redressal commission will be established in each state and district to handle consumer problems at the state level. Six consumer protection rights are included in the Act: (i) protection against the marketing of goods and services that are hazardous to life and property; (ii) information about the quality, quantity, potency, purity, standard, and price of goods or services; (iii) access to a variety of goods or services at competitive prices; and (iv) seeking redress against unfair or restrictive trade practices.[28] This Act makes necessary changes to India's prior consumer protection law; it is progressive and ensures that justice is delivered more quickly. In addition to the Consumer Protection Act 2020, the Indian government has introduced the Consumer Protection (E-commerce) Rules, 2020. It establishes the responsibilities and liabilities of e-commerce platforms, aims to increase e-commerce platforms' transparency and disclosure of information to consumers, and prohibits unfair trade practices in the digital market.[29] The Government of India intends to create a balanced ecosystem for both consumers and sellers through both Acts, which will aid in the expansion of the digital market in India, potentially contributing to the country's GDP.

PERSONAL DATA BILL PROTECTION 2019

The personal data protection bill 2019 was submitted in the Lok Sabha to preserve individuals' data. It applies to data processing by the government, Indian enterprises, and foreign firms, and it includes all businesses under its ambit.[30] Certain data, such as financial data, biometrics, religious or political beliefs, is classified as sensitive personal data,[30] while other data is classified as important personal data.[30] It gives individuals or consumers whose data will be processed the right to ask the entity processing their data how much of their data will be processed, to request correction of inaccurate or incomplete personal data, and to have their data erased, and it emphasizes the importance of consent. If an individual withdraws their consent to allow for the transfer or processing of their data, the commercial entities or other relevant bodies are no longer able to use it. This compels all entities to adopt organizational adjustments to provide better data protection by requiring them to obtain the user's consent before processing or transmitting their data. The bill requires social media intermediaries with a large number of users to include a voluntary user verification mechanism for users in India.[29] All sensitive and critical personal data must be stored in India and cannot be transferred to other countries, according to the bill. Sensitive Personal information can only be transmitted outside of India if it meets the same standards as the General Data Protection Regulation. This bill also calls for the creation of a Data Protection Authority to help safeguard individuals' interests, prevent data misuse, and promote transparency and conformity with the law. It stipulates that the government has the authority to request any valuable non-personal data from corporate entities for sharing. It also specifies the consequences for individuals who break any of the law's provisions. The government's goal with this bill is to ensure that people's data is protected and that it is not misused by a corporate organization.

NEXT STEPS

Technology has become the way of the world in today's globe, and it will only continue to grow in the future, resulting in a higher number of digital platforms and an increase in the number of online consumers. As a result, to keep the market balanced, both the government and business organizations must recognize the value of data and provide a safer marketplace for consumers.

Government

By 2022[31], the Indian digital economy is predicted to exceed $1 trillion, implying a bigger number of e-commerce platforms and hence more data collecting. The Personal Data Protection Bill was introduced by the Indian government to safeguard, control, and prevent the exploitation of its citizens' data. Through this bill, the government hopes to make it essential for all enterprises operating in India to comply with the law. This law is a step forward in promoting greater transparency and citizen data protection. It also prohibits the transfer and use of sensitive data without the user's authorization.

The government emphasizes the need for consent because people's right to privacy is now a basic right, and they can withdraw, erase, and correct any personal information submitted to businesses. The bill exempts the government from the law's scope when it comes to data collecting for official purposes. The government collects and keeps data for a variety of reasons, such as storing

Aadhar information for all Aadhaar cardholders with the Unique Identification Authority of India, then monitoring it through the Central Monitoring System, the National Social Registry, and other means. The government allows these entities to collect and store data since it is for the public's benefit. Even though data is gathered to maintain a database of its inhabitants and for their welfare, this bill has a limitation that exempts agencies from obligation. These agencies should inform citizens about how their data will be used and for what purposes. The Arogya App was created recently to raise awareness about Covid-19. Citizens were forced to disclose personal information to the app, which the central government had access to. However, citizens' minds are still clouded by a lack of understanding about how long the data will be stored, which agencies will have access to it, and who designed the application. Citizens expect the government to provide them with the information they require under the Right to Information Act of 2005 (hence referred to as RTI) in such cases. The Right to Information Act was enacted for the government to be more accountable to citizens' requests for information. It is also believed to work in tandem with privacy regulations, as both aim to make the government more visible and accountable to its citizens. Even though the RTI Act was met with enthusiasm, it appears to be dying slowly over time. According to statistics, between 40 and 60 lakh RTI applications are filed each year, but only approximately 45 percent of those who file them obtain the information they requested.[32] The State Information Commission is still dealing with 2.18 lakh appeals and complaints. The government has also turned down applications relating to demonetization and the recently established PM-Care fund for the Covid-19 pandemic.[33] Rejection of applications and lack of responsibility on critical issues have instilled distrust and ambiguity in citizens' perceptions about the government's actions, which is one of the causes for the low number of RTI applications filed.[33] Today, the government must develop policies for governmental agencies as well, so that individuals' right to information is respected and legitimate questions are answered. So they can rest assured that their personal information is safe with the government. This will also ensure that the government is more transparent and answerable in its approach. The government can also refer to the privacy laws of other countries, like the GDPR, and embed stricter rules favorable to India. The Consumer Protection Act 2019 is also a positive step that will help the government to have stringent control over the platforms on the digital market and create a safer environment for digital consumers. Also, the government must ensure that the laws enacted by it are properly complied with by the Businesses and other authorities.

Business Organization

With the growing amount of e-commerce on digital platforms, there is a paradigm shift of the consumers from offline to online market.[10] At the same time, consumers now have various options and platforms to look for. Hence there is always competition among these platforms to attract the attention of a greater number of consumers. In today's time, consumers are slowly becoming more aware of their data being used by these platforms. Through documentaries and articles, consumers are understanding how they are being lured into providing their data which can further act as a possible threat for them. Hence consumers are getting smarter and more careful about their data. So, for organizations on digital platforms to retain consumers it is pertinent for them to assure their consumers that the data they provide is safe and is not misused by them. For example, Apple in the case of the Federal Bureau of Investigation-Apple Encryption dispute won the trust of its consumers by ensuring that their data is safe and not even Apple can access it. It was after this that it was able to attract and retain more consumers. In this particular case, the FBI had asked Apple to decrypt an iPhone owned by one of the perpetrators in the 2015 San- Bernardino attack.[34] Since Apple does not have any feature to decrypt, they refused to do. For that, the FBI filed a case requesting the court to order Apple to create a custom operating system to hack iPhones by disabling the key security features in iPhones. Apple opposed this order stating it to be unlawful and it would pose a potential threat to the data of all its users. The Chief Executive Officer of Apple, Mr. Tim Cook stood by his stand and for this, the company gained a large number of supports from its users, eventually, the company was able to win the trust of the consumers.[35] Therefore, even if Apple products are more expensive than other brands in the market, the trust factor drives them more consumers. This is an example of how organizations can gain the trust of their consumers by being transparent and true to them. Business organizations should adopt changes to ensure better protection of their consumers' data. They should adopt the process of perturbation to help preserve the useful information in the original data collected from the consumers and at the same time reduce the opportunity for any invader to violate privacy.[36] Moreover, the companies can synthesize data required for their marketing purposes from the original data, this will ensure the protection of the original data and prevent the loss of information.[36] They should make their consumers aware of how their data is being processed and how safe their data is with the organization. Companies should provide safe and secure payment mechanisms and pair up with secured platforms for payments, to prevent frauds and scams. They should consider taking the consent of their consumers before using their data for any major purposes and finally should take measures to ensure that there is no misuse of consumers' data on their part. One more important point would be to inculcate the use of single sign-on authentication.

Single Sign-on authentication

Single Sign-on Authentication is an online service that will help users to log in to multiple platforms using a single login in detail that is using one username, one login Id, and one password.[37] This will simplify the process of login and will also add an extra layer of protection. It will help companies to manage privacy on their platforms as this service will reduce the security risks for consumers and vendors.[37] Companies can strengthen their identity protection. Users can create one strong password and use it on multiple platforms, this will save reduce password fatigue and simplify password management.

EMPIRICAL STUDY ON CONSUMER AWARENESS AND ITS ANALYSIS

To understand the awareness among consumers, we conducted an empirical survey. For the study 20 individuals, across different age groups were questioned to understand their awareness about data privacy and the laws relating to it. The first question put to them was the time they spend on the internet on an average in a week. To this, the answer varied from 12hrs in a week to all the time every single day. Second, they were as to what all they use the internet for, about 30 percent of them responded that they use it for educational work, 30 percent for entertainment, 5 percent for online shopping, and 75 percent for all three. Third, they were asked about their preferred type of market and the reason for the same. 70 percent of the individuals who responded prefer the online market over the offline market because it is easy and convenient to access, good quality products at a discounted price, save time, variety of products in one platform, a wide range of options, and easy to exchange. Next, they were asked about the issue of data privacy. The first question put to them was how concerned they are about their security and privacy on these platforms, 50 percent of the individuals responded that they were very much concerned about their security and 50 percent of them are slightly concerned but not to a larger extent. Then about 35 percent of the total individuals who responded answered that have been the victim of online frauds and about 40 percent of such victims avoided using the application or the website, 40 percent of them registered a complaint with the concerned authority and 10 percent of them contacted the bank to close their accounts to prevent any more loss of money. They were then asked if they have been ever asked to provide their personal information on the e-commerce platforms they visited, to this 85 percent replied in positive, then they were asked as to how many times they refused to give their data, to this question 40 percent answered that they always refuse to give out their data, 50 percent responded that they refuse sometimes and 10 percent responded that they never refuse to give out their data to the e-commerce entities. When asked the reason for refusing to give their data, 55 percent of them responded that they do not trust the organizations with their data, 40 percent of them answered that the websites that ask for their data do not disclose them as to how they plan to use their data, and some believed that the information asked is not proportional to the service provided by the particular websites. Thereafter they were asked the measures that they take to protect their security and data on these platforms, some replied that they check the authenticity of the website before using it, some permit data only if it is mandatory, some keep strong passwords, some of them disclose bank details only on trusted websites, refrain from giving personal data and phone numbers on any website, and use a data protection software and install antivirus, and some just avoid using the internet as much as possible. Then they were questioned on their awareness about the recent consumer protection act 2020 and the data protection bill 2019, only 40 percent of them are aware of the consumer protection act 2020 and 60 percent do not know of it, the latter question only 45 percent of the total individuals who responded are aware of the data protection bill 2019.

The first part of the survey involved questions relating to the usage of the internet and the preference of the individuals on the types of market. From the responses, it is clear that the majority of them are regular users of the internet and prefer online markets over offline markets. As discussed above and also observed through this survey that convenience, versatility, cost, and timesaving are the major factors that drive consumers towards the online market.[14] The second part of the study involved questions relating to consumer awareness. It was observed that though the individual as consumers is concerned about their online security and data privacy, they do not take any major step to address their concern. For example, people who have been a victim of online fraud, most of them avoided using the application or website instead of filing any complaint. This indicates that maybe there is a lack of awareness about the procedure to file a complaint or that they did not want to indulge in any resolution mechanism, hence they preferred to avoid it. Instead of avoiding such frauds, consumers should take the right actions or file a complaint at the website where such fraud was committed so that the organizations are aware of it and this will also alert other consumers. Most of the individuals who responded refrain from giving their data because there is a lack of clarity on how their data will be processed by the companies and for this reason, they do not trust the companies with their data. This points towards the lack of trust the consumers have in the companies asking for their data and they think that companies should be more transparent and clearer about the usage of their data. This is a good sign because consumers understand that they have a right to know what happens to their data, at same time most of them take precautions and measures from their side to protect their data as far as possible, but even after that, there seems a lack of awareness among these individuals about the laws governing data privacy and consumer protection in the country. This may be because the laws are relatively new, and the data privacy bill has not been passed yet but at the same time, consumers should keep themselves informed about the laws so that they understand how they can address issues relating to privacy and consumer protection and the authority they can file their complaint with. This also indicates that since online consumerism is increasing in India, the government should take major initiatives to aware its citizens of the relevant laws on these issues. It is important that consumers become more aware of what they do with their data on the digital platforms and that the companies are obligated to provide them with information about the usage of their data.

CONCLUSION AND SUGGESTIONS

- The world is changing and is moving more and more towards digitization. It is now more of a technology-driven world than it was earlier. The introduction of various technologies has made human lives more convenient and easier, and it is true to say that technologies will govern the future. In this paper, we have briefly discussed one of such technologies that have been adopted widely, which is Artificial Intelligence. AI, as explained above, is very dynamic and functions very similarly to that of a human mind. It performs cognitive tasks that require human intelligence with precision and accuracy. This is the very reason for its acceptance across various sectors. Big companies have also adopted AI to develop personalized products like smart devices, virtual

assistants, etc. These products help to perform various day-to-day activities which make human life easier and faster. Thus, the innovation of AI has proved to be helpful for humans. The next part of the paper explains how the use of AI has impacted consumerism. In this, we tried to explain the power of aggregators like Amazon in influencing consumer behavior by making strategies through the use of AI to attract consumers and successfully retain their consumer base. Strategies like prime delivery & personalized product recommendations have worked in their favor and have helped them to gain more control in the digital market as compared to their competitors. And through rigorous advertisements promoting the quality of their products and services, they can lure consumers into buying their products. Then we discussed the concept of entity resolution, where various data points of individuals like their personal information, political affiliations, etc., are stored in one database which companies to understand all consumer's individual choices and interests. This way they can cater to the individual needs of the consumers and expand their consumer base. Sometimes these user data or consumer data are exploited by business giants for their benefits, for example how Facebook helped Cambridge Analytica by providing personal data of 87 million users to help them in the 2016 presidential election campaign. This exposed the dark side of such huge platforms that lures consumers in providing their personal information which is then converted into precious commodities by these companies. This explains that with every new development there come some serious challenges. Consumer data privacy and security is one such concern faced by consumers all over the world. In India, the digital market is growing at a faster rate, welcoming multiple e-commerce platforms to establish their businesses. Due to the increase in digital platforms, there is a shift of consumers from offline to online markets. My empirical study also suggested that most individuals prefer online markets over offline markets as it is more convenient, easy, and timesaving. It is also true that online businesses have put in efforts to make it more adaptable and convenient for the Indian consumers, like search options available in regional languages, voice search options, etc. with multiple platforms online there is a huge accumulation of data which acts as a potential threat to consumer's data. Unlike in other developed countries like the United States of America and the United Kingdom where consumers are aware of their legal rights, in India due to low literacy, there exists a lack of awareness among the consumers about legal rights. In the empirical study on consumer awareness discussed above, it was observed that when faced with any online frauds or scams, they simply avoid using the application or website instead of taking any active actions. Also, the majority of the individuals who responded, even though all of them knew about data protection and security but most of them were unaware of the laws governing it. This is the area of concern because unless consumers are themselves not aware of their rights, they will not be able to tackle the issues of data privacy and consumer exploitation. One of the major reasons for such unawareness was because there was no law protecting the digital consumers, but now the government has enacted the Consumers Protection Act 2020 and the Consumer Protection (E-commerce) Rules 2020, which provides online consumers with their necessary rights, relief, and a platform to file their grievances. This law is expected to ensure better protection and security of digital consumers and will prevent their exploitation by the business giants. The Personal Data Protection Bill 2019 also lays down strict guidelines to protect the interest of the individuals and punish the business or e-commerce violating any of its provisions. This is a positive step that will not only ensure a better ecosystem for digital consumers but will also make them more aware of their rights. Companies or business organizations should modify or change their policies for better protection of their consumer data, take steps to preserve the original data provided to them and be more accountable to their consumers. The Government should also ensure that the companies comply with the required laws, create more awareness about the consumer protection laws among the citizens through the help of NGOs, etc. In the end, it is only through the cooperation and contribution of the Government, Companies, and Consumers that will help ensure a better and safer online market. There is no denying that humans are growing closer and closer to technologies, with this there is an increase in the number of digital platforms and a variety of choices for consumers. Due to affordability, versatility, and convenience consumers are driven more towards digital platforms and this is expected to increase more in the future. With this, there will be a greater number of challenges, but we should not let it outweigh the benefits of digital platforms instead efforts should be to amplify the benefits of new technology and digital platforms. Considering all of the aforementioned characteristics, the General Data Protection Regulation (GDPR) proves to be a major success in terms of improving the privacy and data security of European Union citizens, and it serves as an ideal role model for other countries seeking to strengthen their data protection laws for the benefit of their citizens.

Personal information can be used to exploit a person's reputation, influence our decisions, and shape our behaviors. It is critical that we protect our personal data and information from third parties. For example, recent data breaches by major service providers such as Facebook and Twitter, among others, have raised serious concerns about whether an individual's personal information is safe or not. The Cambridge Analytica scandal, in which millions of Facebook users' data was leaked and allegedly misused by Cambridge Analytica (a data mining firm linked to Donald Trump's Presidential campaign), sparked outrage around the world, including in India, which has one of the highest Facebook user populations. Because of instances like this, it is critical for a country to have better and stricter data protection regulations, as the more information about us that someone has, the more power they can wield over us.

REFERENCES

[1] G. Tecuci, "Artificial intelligence," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 4, Mar. 2012, doi: 10.1002/wics.200.

[2] H. Xianhong, B. Neupane, L. F. Echaiz, P. Sibbal, and M. Rivera Lam, *Steering AI and advanced ICTs for knowledge societies: a Rights, Openness, Access, and Multi-stakeholder Perspective - UNESCO Digital Library*, 1st ed. UNESCO, 2019. Accessed: Feb. 16, 2022. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000372132

[3] A. Pavaloiu, "The Impact of Artificial Intelligence on Global Trends," Dec. 2016.

[4] S. Srivastava, “Artificial Intelligence: way forward for India,” *Journal of Information Systems and Technology Management*, vol. 15, pp. 1–23, May 2018, doi: 10.4301/S1807-1775201815004.

[5] P. Harvey, E. Currie, P. Daryanani, and J. Augusto Wrede, “Enhancing Student Support with a Virtual Assistant,” Jan. 2016, vol. 160, pp. 101–109. doi: 10.1007/978-3-319-28883-3_13.

[6] S.-C. Necula, “Deep Learning for Distribution Channels’ Management,” *Informatica Economica*, vol. 21, pp. 73–84, Dec. 2017, doi: 10.12948/issn14531305/21.4.2017.06.

[7] Firstpost, “The aggregator model – rise, challenges, and scope of this approach in India-Business News,” *Firstpost*, Jan. 03, 2017. https://www.firstpost.com/business/biztech/the-aggregator-model-rise-challenges-and-scope-of-this-approach-in-india-3728527.html (accessed Feb. 16, 2022).

[8] D. Bednall and M. Valos, “Marketing research performance and strategy,” *International Journal of Productivity and Performance Management*, vol. 54, pp. 438–450, Jul. 2005, doi: 10.1108/17410400510604575.

[9] C. Opia, “Outside-In Marketing Strategy: The Case of Amazon,” Feb. 2021.

[10] C. Fontanella, “20 Customer Touchpoints That Will Optimize Your Customer Journey,” 2020. https://blog.hubspot.com/service/customer-touchpoints (accessed Feb. 16, 2022).

[11] Dun and Bradsheet, “Why Business Entity Resolution is Critical to a Master Data Framework,” 2020. https://www.dnb.com/perspectives/master-data/business-entity-resolution-with-master-data-management.html (accessed Feb. 16, 2022).

[12] I. Lapowsky, “How Cambridge Analytica Sparked the Great Privacy Awakening,” *Wired*. Accessed: Feb. 16, 2022. [Online]. Available: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

[13] K. Vulusi, “E-commerce Growth in India: a study and the potential of its future,” Dec. 2020.

[14] Consultancy, “Bain and Flipkart foresee 350 million online shoppers by 2025,” Jun. 29, 2020. https://www.consultancy.in/news/3139/bain-and-flipkart-foresee-350-million-online-shoppers-by-2025 (accessed Feb. 16, 2022).

[15] “India to overtake US as world’s largest e-commerce market: Study,” *The Economic Times*, Dec. 05, 2016. Accessed: Feb. 16, 2022. [Online]. Available: https://economictimes.indiatimes.com/industry/services/retail/india-to-overtake-us-as-worlds-largest-e-commerce-market-study/articleshow/55819926.cms?from=mdr

[16] B. Chakravorti, “Why It’s So Hard for Users to Control Their Data,” *Harvard Business Review*, Jan. 30, 2020. Accessed: Feb. 16, 2022. [Online]. Available: https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data

[17] C. Ryngaert and M. Taylor, “The GDPR as Global Data Protection Regulation?,” *AJIL Unbound*, vol. 114, pp. 5–9, Jan. 2020, doi: 10.1017/aju.2019.80.

[18] D. Savić and M. Veinović, “Challenges of General Data Protection Regulation (GDPR),” Jan. 2018, pp. 23–30. doi: 10.15308/Sinteza-2018-23-30.

[19] P. Voigt and A. von dem Bussche, “Scope of Application of the GDPR,” in *The EU General Data Protection Regulation (GDPR): A Practical Guide*, P. Voigt and A. von dem Bussche, Eds. Cham: Springer International Publishing, 2017, pp. 9–30. doi: 10.1007/978-3-319-57959-7_2.

[20] P. Voigt and A. von dem Bussche, “Practical Implementation of the Requirements Under the GDPR,” in *The EU General Data Protection Regulation (GDPR): A Practical Guide*, P. Voigt and A. von dem Bussche, Eds. Cham: Springer International Publishing, 2017, pp. 245–249. doi: 10.1007/978-3-319-57959-7_10.

[21] Y. S. Van Der Sype, J. Guislain, J.-M. Seigneur, and X. Titi, “On the Road to Privacy- and Data Protection-Friendly Security Technologies in the Workplace – A Case-Study of the MUSES Risk and Trust Analysis Engine,” in *Data Protection and Privacy: (In)visibilities and Infrastructures*, R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert, Eds. Cham: Springer International Publishing, 2017, pp. 241–269. doi: 10.1007/978-3-319-50796-5_9.

[22] E. Kiesow Cortez, “Data Protection Around the World: Future Challenges,” in *Data Protection Around the World: Privacy Laws in Action*, E. Kiesow Cortez, Ed. The Hague: T.M.C. Asser Press, 2021, pp. 269–279. doi: 10.1007/978-94-6265-407-5_12.

[23] P. Voigt and A. von dem Bussche, “Enforcement and Fines Under the GDPR,” in *The EU General Data Protection Regulation (GDPR): A Practical Guide*, P. Voigt and A. von dem Bussche, Eds. Cham: Springer International Publishing, 2017, pp. 201–217. doi: 10.1007/978-3-319-57959-7_7.

[24] U. Pagallo, M. Durante, and S. Monteleone, “What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT,” in *Data Protection and Privacy: (In)visibilities and Infrastructures*, R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert, Eds. Cham: Springer International Publishing, 2017, pp. 59–78. doi: 10.1007/978-3-319-50796-5_3.

[25] A. G. Awesta, “European Laws’ Effectiveness in Protecting Personal Data,” in *Data Protection Around the World: Privacy Laws in Action*, E. Kiesow Cortez, Ed. The Hague: T.M.C. Asser Press, 2021, pp. 249–267. doi: 10.1007/978-94-6265-407-5_11.

[26] C. Bier, S. Kömpf, and J. Beyerer, “A Study on Corporate Compliance with Transparency Requirements of Data Protection Law,” in *Data Protection and Privacy: (In)visibilities and Infrastructures*, R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert, Eds. Cham: Springer International Publishing, 2017, pp. 271–289. doi: 10.1007/978-3-319-50796-5_10.

[27] R. K. Bangia, *Consumer Protection Act*. ALLAHABAD LAW AGENCY, 2018.

[28] B. Viswanathan and A. K V, “A Study on Consumer Protection Act 2019 and Its Implications on the Pillars of Integrated Communication Channel,” Sep. 2021, doi: 10.9790/487X-2309055967.

[29] Department of Consumer Affairs, *Consumer Protection (E-Commerce) Rules Government of India*. 2020. Accessed: Feb. 16, 2022. [Online]. Available: https://consumeraffairs.nic.in/theconsumerprotection/consumer-protection-e-commerce-rules-2020

[30] R. Singh and S. Ruj, *A Technical Look At The Indian Personal Data Protection Bill*. 2020.

[31] S. Shaily, “Data-Privacy Concerns and Its Influence on Consumer Purchasing Intention in Bangladesh and India,” *International Journal of Marketing Studies*, vol. 13, p. 26, Jan. 2021, doi: 10.5539/ijms.v13n1p26.

[32] M. Chhibber, “In 15 years, RTI has gone from Indian citizens’ most powerful tool to an Act on life support,” *ThePrint*, Jun. 24, 2020. https://theprint.in/opinion/in-15-years-rti-has-gone-from-indian-citizens-most-powerful-tool-to-an-act-on-life-support/447507/ (accessed Feb. 16, 2022).

[33] K. S. Kumar, “Opinion | The paradox of our rights to information and privacy,” *mint*, Dec. 11, 2019. https://www.livemint.com/opinion/online-views/the-paradox-of-our-rights-to-information-and-privacy-11576085219492.html (accessed Feb. 16, 2022).

[34] L. Kahney, “The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No,” *Wired*. Accessed: Feb. 16, 2022. [Online]. Available: https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

[35] Q. Zhang, “Research on Apple Inc’s Current Developing Conditions,” *Open Journal of Business and Management*, vol. 06, pp. 39–46, Jan. 2018, doi: 10.4236/ojbm.2018.61003.

[36] S. Gupta and M. J. Schneider, “Protecting Customers’ Privacy Requires More than Anonymizing Their Data,” *Harvard Business Review*, Jun. 01, 2018. Accessed: Feb. 16, 2022. [Online]. Available: https://hbr.org/2018/06/protecting-customers-privacy-requires-more-than-anonymizing-their-data

[37] T. Bazaz and A. Khalique, “A Review on Single Sign on Enabling Technologies and Protocols,” *International Journal of Computer Applications*, vol. 151, pp. 18–25, Oct. 2016, doi: 10.5120/ijca2016911938.