
CONSUMER CONSENT AND DATA MONETIZATION PRACTICES IN DIGITAL BUSINESS MODELS

Vaishnavi Bhoi, B.A. LL.B., Manikchand Pahade Law College, Chhatrapati
Sambhajanagar, Maharashtra, India

ABSTRACT

In today's digital age, online platforms collect and use large amounts of consumer data for various purposes such as advertisements, marketing, and other business purposes. Although these practices help companies to improve their services, they also raise concerns regarding privacy, transparency and misuse of personal information of users. This paper examines consumer consent and data monetization practices in digital business models with special focus on privacy and protection of personal data.

This study was conducted using doctrinal research method. The secondary sources employed include articles, laws, websites, and judicial precedents. Legal principles of data protection in India have been examined in this paper. In addition, there has been consideration of various international laws including General Data Protection Regulation. Some of the landmark judgments and challenges on issues of meaningful consumer consent in the digital world have also been discussed.

From the discussion, it can be concluded that protection of consumers' privacy through legal frameworks, transparency and consumer education is imperative.

Keywords: Consumer Consent, Data Privacy, Data Monetization, Digital Platforms, Consumer Rights, Privacy Policies, GDPR, DPDP Act, Digital Privacy, Data Protection.

1. Introduction

People of today's time use various mobile apps, websites, and social media platforms in their everyday routine. Companies gather various data of consumers such as their names, phone numbers, emails, their location, online search history, and various preferences and interests. Consumer data is highly valuable for companies as it can be used for advertisement purposes and earn revenue out of it.

While using websites and apps, companies ask for consumer consent through privacy policies, cookies, and terms and conditions of service. In most of the cases, consumers do not pay attention to these terms and click the "Accept" button blindly without knowing its actual meaning. This brings an important question in mind that whether consumer understands the terms of privacy policies while accepting them.

Companies often use consumer data for giving them personalized advertisements and recommendations based upon their online behaviour. At times, this proves to be helpful for users whereas, in other instances, it violates privacy and misuse of consumer data and raises concerns. There is a definite requirement of strong and efficient laws for the protection of consumer data and privacy. In India, the right to privacy was acknowledged by the case of Justice K.S Puttaswamy v. union of India. The Digital Personal Data Protection Act was also brought in for the protection of personal data. International laws such as the General Data Protection Regulation also play an essential role in the protection of the privacy of the consumers.

This paper analyses consumer consent and data monetization practices in digital business models. It also describes the legal framework of data protection and the challenges of protecting the privacy of the consumers in the digital age.

2. Literature review

In recent years the issues of consumer consent and data monetization has become an important area of discussion. Various scholars, legal experts, courts, and regulatory authorities have examined or studied these by examining relationship between consumer privacy, consumer consent and business models.

One of the most significant contributions to this field is by Shoshana Zuboff in *The Age of*

Surveillance Capitalism.¹ Zuboff explained that how this digital companies uses personal data of consumers to predict and influence consumer behaviour. According to her, this companies uses this data to generate profit by analysing and monetizing user information. Her work raised a concern about the excessive use of personal data and increasing imbalance between consumers and digital corporations.

Another important contribution is made by Daniel J. Solove, who discusses the limitations of consent-based privacy protection.² Solove has stated that most of the users don't even read or fully understands what are the policies and blindly gives there consent. And as a result, consumes don't even know that how there data is being collected, processed and even shared. He also suggests that only relying on consent will not solve this problems because the policies, cookies are too lengthy and hard to understand.

Some studies have examined the role of the General Data Protection Regulation (GDPR) of the European Union in strengthening data protection³. Scholars have observed that the GDPR introduced important principles such as informed consent, transparency, accountability, purpose limitation, and the right of individuals to control their personal data. GDPR is often considered as one of the strongest data protection mechanisms in the world. And it has influenced many countries.

In India, the discussion on privacy and data protection gained significant importance after the Supreme Court's decision in *Justice K.S. Puttaswamy v. Union of India*.⁴ The judgment recognized privacy as a fundamental right under Article 21 of the Constitution of India. This has been considered a major decision by some of the scholars and a step towards the development of privacy law in India.

The Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna also played a crucial role in shaping the debate on data protection in India.⁵ The Committee mainly focused on the importance of informed consent, transparency, accountability, and protection of personal data. It also highlighted the need for a comprehensive legal framework

¹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

² Daniel J. Solove, *Understanding Privacy* (Harvard Univ. Press 2008).

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016, 2016 O.J. (L 119) 1.

⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.

⁵ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

which should be capable of balancing technological innovation with individual privacy rights.

Moreover, some recent studies have investigated the issue of the use of dark patterns in digital platforms as well. Dark patterns can be described as design features that affect a user's decision and make him/her do something certain on the Internet.⁶ Such things include accepting terms and conditions of using the platform, accepting cookies, or providing one's personal data, among other similar things. Generally speaking, it is believed that dark patterns affect one's free decision-making process. Thus, it is questionable whether the user gave his/her consent voluntarily or not.

The issue of Cambridge Analytica was also an important reminder about data privacy and consumers' rights.⁷ From the analysis and research conducted in connection with the scandal, it became clear how the private data of social media users can be exploited for political marketing and manipulation.⁸ This scandal has raised a number of very important questions about the manner of collecting and storing of such data by commercial enterprises.

Despite extensive research conducted in the areas of privacy, data security, and consumer rights, there are still certain topics that call for deeper investigation. For example, it should be determined whether consumers properly understand the implications of giving consent during their use of various online applications and the ways in which their data is utilized by firms. It is for this reason that the current research is focused on studying the problem of consumer consent, data monetization laws, and data protection policies in India.

3. Research Methodology

The following research paper makes use of doctrinal research methodology to explore the issue of consumer consent in relation to the practice of monetizing consumer data within digital business models. The doctrinal approach to research methodology is largely concerned with the examination of legal sources like laws, judgments, documents, journal articles, among others. It is ideal for the current research because the study will be focusing on the legal

⁶ Role and Challenges of User Consent in Social Media, Journalism University, <https://journalism.university/social-media-and-society/role-challenges-user-consent-social-media/> (last visited June 13, 2026).

⁷ Issie Lapowsky, How Cambridge Analytica Sparked the Great Privacy Awakening, WIRED (Mar. 17, 2019), <https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>

⁸ Carole Cadwalladr & Emma Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, THE GUARDIAN (Mar. 17, 2018), <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

framework surrounding the data protection of consumers.

Most of the data used in the research is secondary in nature. The sources used in the research include the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, decisions of the Indian Courts, official publications from the government, books from academics, peer-reviewed journal articles, and online sources that are authentic. A special emphasis is made on the decision in Justice K.S. Puttaswamy v. Union of India, where the court held that privacy is a fundamental right under the Indian Constitution.

Apart from doctrinal research, another limited approach of comparison has been utilized. The comparison of some issues concerning the Indian law regime with GDPR has been made. Such a comparison is helpful for comprehending the global standards associated with obtaining informed consent, ensuring transparency, and data protection. Moreover, it offers valuable lessons on how privacy laws can be enhanced to counter issues posed by modern digital business practices.

The aim of the methodological approach in this study is to examine the legal norms that have been laid down, understand the difficulties related to obtaining informed consent from consumers, and determine if there is sufficient protection offered through such legislation against any abuse of personal data. The study will try to examine the existing data protection norms in light of legal precedents and literature.

4. Consumer Consent in digital platforms

Consumer consent refers to the permission given by the user to the company to use and collect their personal data. With the increasing usage of internet and mobile apps, people today use various mobile applications, websites, and social platforms daily.⁹ While using these platforms, the users may be asked by the company to share their data such as name, contact number, email address, location, photos, and online activities. Users' consent is taken for sharing this information.

The consent of digital platforms is taken from users regarding privacy policy, cookie notice, and terms and conditions. There is always some type of option pop-up like 'Accept', 'Allow

⁹ Stripe, What Is Consumer-Permissioned Data? Here Is How to Use It and Why It Is So Important, <https://stripe.com/in/resources/more/what-is-consumer-permissioned-data-here-is-how-to-use-it-and-why-it-is-so-important> (last visited May 23, 2026).

Access' and "Agree to terms and conditions". Most of the applications and websites ask users to allow access to their camera, contract, microphone, and location. But majority of the users click on these options without properly and effectively knowing all details due to their complexity.

There is a major issue involved in all of this. Consumers usually don't understand how their private data is being stored, collected and used by the company. Many times, the private information is being used for advertising and marketing purposes without properly making it clear to the consumer. As a result, one question emerges here that whether the consumer's consent is true? This happens in many cases where users simply give their consent without knowing anything about the data practices.

Informed consent of consumers holds great importance when it comes to maintaining privacy and consumer rights.¹⁰ It is necessary that consumers must understand the nature of their data which is being shared and for what purpose this will be used. The company must have clear and understandable privacy policies so that everybody can easily comprehend it. This is because proper consent from the users helps establish trust between the consumer and the digital platforms. In addition, the user's personal data becomes safe from misuse by other entities.

5. Data monetization practices in digital business models

These days, a large number of digital organizations are earning money through the acquisition and exploitation of consumer data, which is called data monetization. Data monetization can be done by selling data to any other company or by exploiting it within innovative work opportunities. Data like search history, purchasing behaviour online, location, interests, activities on social media allows organizations to analyse consumer behaviour.¹¹

A number of digital organizations make use of consumer data in order to offer advertisements based on consumer behaviour and preferences¹². As an example, if someone makes a search for clothes or watches videos of some products, he/she will start seeing advertisements related

¹⁰ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

¹¹ Talend, Data Monetization, <https://www.talend.com/resources/data-monetization/> (last visited May 22, 2026).

¹² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

to their needs suddenly pop up on different mobile applications. The main goal of digital organizations in this way is to attract more customers and generate higher revenue.

Digital business models primarily rely upon data-driven services. Social media platforms, e-commerce websites, video streaming applications, and online search engines gather enormous amounts of user data on a daily basis. Apart from this, companies also tend to share their consumer's data with third parties for promotional and marketing purposes. Even if these practices enhance the quality of service offered to consumers, it raises serious privacy concerns.

Despite the above, such actions have some disadvantages in terms of privacy violation and exploitation of personal information.

With the increase in the use of customer data for business purposes, the problem of legality and ethics of data exploitation has become a big one. Not everyone is aware of how companies exploit their data for various benefits. There may be implications on the privacy and freedoms of consumers in case of too much information exploitation. Hence, there is an urgent need for legislation and awareness on the part of consumers.

6. Legal framework governing data privacy and consent

6.1 Indian legal framework

It has become very essential to protect individuals' data and privacy. Individuals are sharing a huge amount of personal information on different online platforms such as social media platforms, e-commerce sites, and even mobile apps. With respect to increased consumer data usage, it has become necessary to have appropriate regulations for protecting individuals' privacy and collecting data.

The right to privacy was made a fundamental right by the Supreme Court of India in the case of Justice K.S Puttaswamy v. Union of India. The court observed that the right to privacy was one of the most important aspects of Article 21 of the Indian constitution. Such decisions made by the court acted as a landmark judgement for privacy protection in India.

India also passed the Digital Personal Data Protection Act that regulates data and its usage¹³.

¹³ Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

It focuses on DPDP Rules, 2025 which are about the process of collecting, processing, and protecting personal data.¹⁴ There are also laws regarding the safety and security of digital information in the IT act 2000.¹⁵ These laws ensure that proper rules can be followed in the online world.¹⁶

6.2 GDPR and international perspective

The General Data Protection Regulation (GDPR) is one of the main legislative acts regarding issues of data protection and privacy.¹⁷ The GDPR is an EU and EEA data privacy law, which grants the citizens of European Union and European Economic Area jurisdictional powers over processing of personal data either digitally or manually.¹⁸

This legislation ensures several consumer rights, including the rights to access personal data, modify information, and delete personal data under some conditions. This law requires companies to obtain proper and informed consent of consumers before processing their personal data.

In contrast to GDPR, the data privacy policy in India is still forming. Despite all of that, the need for the privacy of the consumer along with responsibility and transparency in dealing with personal data in the digital business sphere cannot be overlooked even in India or outside it.

7. Judicial approach and imp case laws

The Indian judicial system has also been very significant in safeguarding privacy and personal data in the digital age. As digital technology and social media platforms were increasingly being used in daily life activities, courts understood their implications on data protection and privacy of citizens. By making various rulings, courts have always attempted to safeguard the rights of individuals and use personal data responsibly.

¹⁴ EY, Decoding the Digital Personal Data Protection Act, 2023, https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 (last visited May 22, 2026).

¹⁵ Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

¹⁶ PRS Legislative Research, Digital Personal Data Protection Act, 2023, <https://prsindia.org> (last visited May 25, 2026).

¹⁷ Teodor Stanciu, GDPR for dummies, Termly (may. 22 2026, 6.14pm) <https://termly.io/resources/articles/gdpr-for-dummies/>

¹⁸ European Commission, Data Protection Rules in the European Union, https://commission.europa.eu/law/law-topic/data-protection_en (last visited May 25, 2026).

Such a judgment comes from Justice K.S Puttaswamy v. Union of India¹⁹. The case involved a matter of apprehension about the protection of data and the privacy of citizens through the Aadhar Card scheme. The concern that came to light before the Supreme Court was whether or not privacy was a fundamental right guaranteed by the Constitution of India. According to the judgment of the Supreme Court, privacy was indeed a fundamental right provided for by Article 21 of the Constitution of India. Such a landmark judgment was one of the stepping stones towards data and privacy protection.

Another significant case to mention is Karmanya Singh Sareen v. Union of India.²⁰ It followed WhatsApp's announcement of a privacy policy that would include user data sharing with Facebook. Petitioners in this case contended that consumers were not sufficiently aware about their personal data collection and sharing. These cases are of relevance due to the issue of informed consumer consent and privacy of users' data on digital platforms. Despite the fact that the court was unable to prevent the enforcement of the privacy policy, this case significantly boosted the level of consumer interest in digital privacy. There is a greater necessity for better data protection regulations in India.

Cases described above show the rising importance of issues such as privacy and informed consumer consent.

8. Challenges in meaningful consumer consent

One of the main challenges in the digital world is that the consumer provides consent without proper knowledge of privacy policies and terms and conditions. According to the research by Pew Research Centre carried out in 2019, only 9 % of adults read privacy policies and terms of service agreements before agreeing to them with an "I agree" button.²¹ The users tend to hit the "Accept" button without knowing how their personal data would be used and exploited by the company. Thus, the consumer consent is not always informed.

Transparency issue is one more challenge in digital platforms. Companies cannot provide full information about their data collection methods, and users cannot have any control over their

¹⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

²⁰ *Karmanya Singh Sareen v. Union of India*, S.L.P. (C) No. 804 of 2017 (India).

²¹ Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> (last visited May 24, 2026).

data. At the same time, digital platforms also make use of tracking technologies and cookies to analyse consumer behaviour for advertising and marketing purposes.

Another challenge relates to the digital literacy level of users.²² The consumers do not know much about their privacy rights and relevant laws. Hence, consumers require easier to understand privacy policies and regulations, increased digital literacy and strict regulations.

9. Suggestions and reforms

It is recommended that the digital platform companies simplify the process of reading privacy policies and terms and conditions, in order to enable consumers understand what they consent to when accessing digital platforms. Most of the users do not take time to go through the long and complicated policies in order to understand them and make an informed decision.

Also, there should be strong enforcement of laws on data protection as well as stricter regulations on digital firms.²³ The firms must ensure that they only collect necessary information from users and also, inform them the reason why the information is required from them. Also, proper penalties must be instituted in the case of violation of user privacy and abuse of consumer data.

Finally, there should be awareness programs on digital privacy and data protection. Programs aimed at educating consumers on how to protect themselves and exercise their privacy rights should also be instituted to enlighten people on their rights on privacy and online safety. They must also be sensitized on how to utilize the available privacy settings in digital platforms.

International collaboration is crucial for consumer protection in the digital era as well.²⁴ It is evident that there are several digital forums operating worldwide, hence it is essential for nations to cooperate for developing better policies for consumer privacy and protection. Legal reform as well as business ethics can contribute towards consumer protection and consent.

²² UNESCO, *Digital Literacy Global Framework: A Reference Framework for Digital Literacy Skills for Indicator 4.4.2* (2018), <https://unesdoc.unesco.org/ark:/48223/pf0000265403> (last visited May 24, 2026).

²³ United Nations Conference on Trade and Development (UNCTAD), *Data Protection and Privacy Legislation Worldwide* (2021), <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (last visited May 25, 2026).

²⁴ Organisation for Economic Co-operation and Development (OECD), *OECD Privacy Guidelines* (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited May 25, 2026).

10. Discussion

The analysis of consumer consent and data monetization practices shows that personal data has become a valuable asset in the digital economy²⁵. Digital companies collect and process large amounts of data about their customers to offer customized services, ads, and business potential. Although this helps in advancing technology and promoting business, it poses a number of important issues related to privacy, transparency, and consumer rights.

The positive aspects in this field is the increasing realization that privacy can be considered a legal right. This was demonstrated by the case of Justice K.S. Puttaswamy v. Union of India, which declared privacy as a fundamental right and laid the foundation for data protection law in India. Another example of this aspect can be observed in the form of the Digital Personal Data Protection Act, 2023, which aims at regulating the collection and processing of personal information.

But still there are several issues that influence the efficiency of consumer consent. Firstly, privacy policies and terms & conditions very lengthy difficult to understand. Therefore, people give consent even if they do not fully understand how the information about them is going to be used. Thus, it is questionable whether consent is really informed.

An additional challenge faced here is that of the lack of awareness on the part of consumers about data privacy and digital rights. Because most of the users don't know how their data is being used and processed by firms. This information deficit leads to an uneven relationship between digital platforms and the consumer.

In order to address these issues, greater importance needs to be given to transparency, consumer awareness, and effective enforcement of laws related to data protection. Privacy statements need to be written in clear and comprehensible language. The collection of data on the part of digital platforms needs to be limited to what is required and proper measures need to be taken to handle personal information responsibly. Regulatory control and consumer awareness programs can also help increase consumer trust in this regard.

²⁵ World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Jan. 2011), https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (last visited May 25, 2026).

11. Conclusion

In the contemporary digital age, the issue of consumer data has taken on increasing importance. Organizations make use of personal information for their advertisements and other purposes as per their business model. Such actions raise several concerns regarding privacy, transparency, and abuse. Consent of consumers plays an important role in ensuring protection of privacy and personal information. However, in most cases, consumers do not understand their privacy policies. Therefore, it is essential that digital platforms provide complete information regarding the collection and processing of consumer data.

The present research was aimed at analysing the topic of consumer consent and the emerging trend of data monetization in the field of digital businesses. The paper discussed the issue of collecting, processing, and using consumers' personal data for business needs by digital platforms. Moreover, attention was paid to the regulation of data protection, namely to such legislative acts as the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and the General Data Protection Regulation of the European Union. Judicial precedents such as the case of Justice K.S. Puttaswamy v. Union of India have been analysed.

However, what the study reveals is the challenge of obtaining genuine consent despite being the key justification in law for personal data processing. It is quite common for privacy notices to be long and hard to interpret due to the many clauses they contain. This makes it challenging for users to appreciate what is expected of them with respect to their information usage.

The research has also shown that the existing legal mechanisms have achieved much success in terms of consumer privacy protection. However, the effectiveness of such privacy protection will be dependent on the implementation of the laws, the regulation of the implementation process, and the awareness of consumers about the privacy issues.

To conclude, consumer consent cannot be considered as merely a formality but needs to be recognized as a crucial mechanism for ensuring the privacy of the individual. As technology continues to advance into the future, there needs to be cooperation between business, regulatory authorities, and consumers to ensure that development is coupled with privacy preservation.