International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

User Consent and Data Protection: Legal Challenges on Social Media Platforms

Sheetal Ramesh Nikam

PES Modern Law College,Pune

ABSTRACT:

The development and advancements in science and technology have compelled the legislature of countries all over the world to bring new laws into existence. Data Protection laws is one among such laws, which emerged very recently to combat the cyber-attacks against a person's right to privacy. The right to privacy includes the right to protect his/her data too. Nowadays, data privacy and its protection are a concern of every individual due to the misuse of technological developments.

Data Protection is a mechanism that talks about how to protect a person's data from unauthorized access and malicious insiders. Indian constitution being a constitution that gives priority to rights rather than duties had already emphasized the importance of the right to data privacy and its protection impliedly through Art. 21. Even though the Bhartiya Nyaya Sanhita, Information Technology Act, and Right to Information Act talk about it, still India doesn't possess separate legislation for the data privacy and its protection.

The purpose of this research paper is to study the existing legal status of Data Protection laws in India and also to check the current status of the proposed Personal Data Protection Act and the challenges faced by the user in social media platforms regarding consent and data protection.

Keywords: Data Privacy, Data Protection, Information Technology, Personal Data Protection Act.

INTRODUCTION:

Social media platforms have revolutionized the way people communicate, share information, and interact online. From connecting with friends and family to accessing news and entertainment, social media has become an integral part of daily life for millions of people around the world. However, this increased reliance on social media has also raised concerns about data protection and privacy.

User consent is a fundamental principle of data protection on social media platforms. It refers to the permission given by users for the collection, processing, and sharing of their personal data. In the context of social media, personal data can include information such as names, email addresses, location data, and browsing history. Social media companies often collect and process this data to provide personalized services, target advertisements, and improve user experience.

In India, the legal framework surrounding user consent and data protection on social media platforms is primarily governed by the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules). The IT Act provides a broad framework for the protection of personal data and requires entities to collect and processing data to obtain user consent. The SPDI Rules, on the other hand, provide specific guidelines for the collection, processing, and protection of sensitive personal data or information.

Recent privacy scandals, such as the Cambridge Analytica controversy, have highlighted the need for stronger data protection laws in India. In response, the government introduced the Personal Data Protection Act,2023 , which aims to regulate the processing of personal data and protect the privacy of individuals. The Act includes provisions for user consent, data localization, and the establishment of a Data Protection Authority, signaling a significant step towards enhancing data protection and privacy in India.

As the use of social media continues to grow, it is essential to ensure that user consent and data protection remain a top priority. This requires a collaborative effort from policymakers, regulators, and social media companies to create a legal framework that protects user data while also allowing for innovation and growth in the digital economy. Only by working together can we create a safe, secure, and ethical environment for social media users in India and around the world.

CONCEPT OF DATA PROTECTION

'Data Protection' talks about a set of privacy laws, policies, and procedures that intend to minimize interference with one's privacy caused by the compilation, storage, and distribution of personal data. Here the word Personal data means any information or data that speaks about a person and he/she can be recognized from that information or data. Normally such data or information will be collected by the Government itself or by any private corporate body or agency. In other words, data protection is a mechanism talking about the protection of data from any unauthorized access. The methods and extent of data protection varies from person to business and business to government accordingly.

LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

Analysis Of Information Technology Act,2000:

Overview of the Information Technology Act, 2000: The Information Technology Act, 2000 (IT Act) is India's primary legislation for governing electronic commerce and data management. It provides legal recognition for transactions conducted electronically, allowing for the electronic filing of documents with government agencies. The Act also amends several other laws, including the Indian Penal Code, the Indian Evidence Act, and the Reserve Bank of India Act, to accommodate electronic records and transactions. The IT Act extends across India and applies to offenses committed outside India as well.1[1]

Salient Features of the IT Act, 2000:

- The Act replaced "digital signature" with "electronic signature" to make it technology- neutral.
- It elaborates on offenses, penalties, and breaches related to cybercrimes.
- The Act outlines the Justice Dispensation System for handling cybercrimes.
- The definition of a cybercafé is included, describing it as any facility offering public access to the internet.
- The Act provides for the constitution of the Cyber Regulations Advisory Committee.
- It amends various statutes, such as the Indian Penal Code and the Indian Evidence Act, to include electronic documents within their scope.
- The Act includes a provision under Section 81, ensuring that its provisions override any other conflicting laws, while not restricting rights under the Copyright Act, 1957.

Amendments Brought in The Information Technology Act, 2000:

- The IT Act introduced amendments in four statutes (Penal Code, Evidence Act, Banker's Books Evidence Act, and the Reserve Bank of India Act) through Sections 91- 94.
- The amendments expanded the definition of "document" to include electronic documents and updated the definition of "Banker's-book" to include printouts of electronic data.
- A significant amendment in 2008 introduced Section 66A, penalizing the sending of "offensive messages," and Section 69, which empowered authorities to intercept, monitor, or decrypt any information through computer resources. This amendment also introduced penalties for child pornography, cyber terrorism, and voyeurism. The amendment was passed without debate and signed into law in February 2009.

Analysis of the Personal Data Protection Act,2023

Overview of the Personal Data Protection Act,2023 : The Personal Data Protection Act,2023 , aims to establish a comprehensive framework for privacy protection in India, emphasizing the rights of data owners. The Act introduces the concept of "digitally enabled consent," ensuring that consent is given in real-time and can be revoked by the data owner at any time. This Act was drafted following the landmark KS Puttaswamy case, which recognized the Right to Privacy as a fundamental right.

Objectives and Key Features:

- The Act aims to secure more rights for data owners, ensure clear and real-time consent, and address the issue of data localization.
- It relaxes norms for cross-border data transfer, though the transfer of critical data remains restricted, with exemptions for health and emergency services.
- The Act retains the roles of the Data Protection Authority and Data Protection Officer, emphasizing the "privacy by design" principle, which must be certified by regulation.

[1] The Information Technology Act, 2000.pdf,
https://i4c.mha.gov.in/theme/resources/actRule/The%20Information%20Technology%20Act,%202000.pdf (last visited Aug 23 2024).

- A new entity, the "consent manager," regulated by the Data Protection Authority, is introduced to help users manage their consent for data processing.

USER CONSENT AND DATA COLLECTION ON SOCIAL MEDIA PLATFORMS

Types Of Data Collected By Social Media Platforms

The collection and use of personal data by social media platforms have become integral to their operations, influencing user experiences, advertising strategies, and even societal trends. This essay delves into the types of data collected by social media platforms, focusing on personal information, demographic information, behavioural data, and device information. It also explores the implications of this data collection for users and society at large.[2]

I. **Personal Information:** Personal information refers to data that identifies or can be used to identify an individual. Social media platforms collect various types of personal information, including:

1. **Name**: Users are typically required to provide their full name when creating an account on a social media platform. This information is used to personalize the user experience and facilitate interactions with other users.
2. **Age:** Platforms often ask for users' age to comply with age restrictions and tailor content accordingly. Age information can also be used for targeted advertising.
3. **Gender:** Users may be asked to specify their gender to personalize content and ads. Gender information is also used for demographic analysis and ad targeting.
4. **Contact Details**: Social media platforms may collect users' email addresses or phone numbers for account verification and communication purposes.

II. **Demographic Information**: Demographic information includes characteristics such as location, language, education, and occupation. Social media platforms collect demographic information to better understand their user base and target ads effectively. Some examples include:

1. **Location**: Platforms track users' locations to provide location-based services, such as local event recommendations or weather updates. Location data is also valuable for targeted advertising.
2. **Language**: Platforms use language preferences to deliver content in users' preferred languages and to tailor ads based on linguistic preferences.
3. **Education and Occupation**: Users may voluntarily provide information about their education and occupation, which can be used for ad targeting and to recommend relevant content.

III. **Behavioural Data**: Behavioural data refers to information about users' actions and interactions on social media platforms. This data is used to personalize content, improve user engagement, and target ads. Examples of behavioural data collected by social media platforms include:

1. **Likes:** Platforms track the content that users like to understand their interests and preferences. This information is used to recommend similar content and target ads.
2. **Shares**: Sharing behavior indicates the content that users find interesting or valuable enough to share with their networks. Platforms use this data to identify popular content and improve content recommendations.
3. **Comments:** Comments provide insights into users' opinions and engagement levels. Platforms use this data to gauge user sentiment and improve content relevance.

IV. **Device information** includes data about users' devices, such as IP addresses, browser types, and operating systems. This information is collected for security purposes, to optimize the user experience, and for targeted advertising. Examples of device information collected by social media platforms include:

1. **IP Address:** IP addresses are used to identify users' devices and approximate their locations. This information helps platforms prevent unauthorized access and fraud.
2. **Browser Type**: Platforms collect data on users' browser types to optimize the user interface and ensure compatibility with different devices.
3. **Operating System**: Information about users' operating systems helps platforms tailor their apps and services to specific devices and improve overall performance.

[2] Katherine N. Lemon & Peter C. Verhoef, Understanding Customer Experience Throughout the Customer Journey, 80 JOURNAL OF MARKETING 69 (2016).

Implications of Data Collection: The collection of personal data by social media platforms raises several implications for users and society, including:

1. **Privacy Concerns**: The vast amount of personal data collected by social media platforms raises concerns about privacy and data security. Users may be unaware of the extent of data collection and how their data is being used.
2. **Targeted Advertising**: Social media platforms use personal data to target ads based on users' interests, behaviors, and demographics. While targeted advertising can be more effective, it also raises concerns about manipulation and privacy.
3. **Algorithmic Bias**: Algorithms used by social media platforms to personalize content and ads may inadvertently perpetuate bias and discrimination, based on the data they are trainedon.
4. **Data Breaches:** The collection of large amounts of personal data makes social media platforms targets for hackers and cybercriminals. Data breaches can lead to identity theft and other forms of fraud.
5. **Regulatory Challenges**: Regulating the collection and use of personal data by social media platforms poses challenges due to the global nature of these platforms and the differing regulatory frameworks across jurisdictions.

Social media platforms collect a wide range of data from their users, including personal information, demographic information, behavioral data, and device information. This data is used to personalize content, improve user engagement, and target ads. However, the collection and use of personal data also raise concerns about privacy, algorithmic bias, and data security

METHODS USED TO OBTAIN USER CONSENT

Privacy Policies: Privacy policies are a key method used by social media platforms to inform users about their data collection and processing practices. These policies outline the types of data collected, how it is used, and how users can manage their privacy settings. Privacy policies are typically accessible through a link on the platform's website or app, and users are often required to agree to the policy when creating an account.

Opt-In Mechanisms: Opt-in mechanisms are used to obtain explicit consent from users for certain types of data processing. For example, when users sign up for a social media platform, they may be asked to opt-in to receive marketing emails or allow the platform to share their data with third parties. Opt-in mechanisms ensure that users actively consent to these activities, rather than having their data collected or shared by default.

Cookie Consent Banners: Cookie consent banners are used to inform users about the use of cookies and other tracking technologies on a website or app. These banners typically appear when a user first visits the site and require the user to consent to the use of cookies before proceeding. Cookie consent banners are designed to ensure that users are aware of and agree to the tracking of their online behavior for purposes such as analytics, advertising, and personalization.

Privacy Settings: Privacy settings are tools provided by social media platforms that allow users to control who can see their posts, what data is collected, and how it is used. These settings enable users to customize their privacy preferences based on their comfort level with sharing information. For example, users can choose to make their profiles public, private, or accessible only to selected friends or followers.

GDPR and CCPA Compliance: Platforms that operate in regions with stringent data protection laws, such as the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), must comply with specific requirements for obtaining user consent. These laws require platforms to obtain explicit consent from users before collecting or processing their personal data and to provide users with clear information about their data rights. Platforms that fail to comply with these laws may face fines and other penalties.[3]

Social media platforms use a variety of methods to obtain user consent for data collection and processing. These methods include privacy policies, opt-in mechanisms, cookie consent banners, privacy settings, and compliance with data protection laws. By providing users with transparent information and control over their data, platforms can help build trust and ensure that user privacy is respected.

CHALLENGES IN OBTAINING MEANINGFUL CONSENT

Obtaining meaningful consent from users for the collection and processing of their personal data is a critical aspect of data protection and privacy. However, there are several challenges in ensuring that consent is meaningful and informed. These challenges stem from various factors, including the complexity of privacy policies, consent fatigue, lack of transparency, limited control over data, and cross-platform tracking. This essay explores these challenges in detail, highlighting their implications for user privacy and suggesting strategies to address them.

Complexity of Privacy Policies: Privacy policies are essential documents that outline an organization's data practices and inform users about how their data will be collected, used, and shared. However, privacy policies are often lengthy, complex, and filled with legal jargon, making them difficult for the average user to understand. This complexity can lead to a lack of comprehension among users, resulting in uninformed consent. To address this challenge,

[3] GDPR and CCPA Compliance: Platforms that operate in regions with stringent data protection laws, such as the EU’s General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), must comply with specific requirements for obtaining user consent.

organizations should simplify their privacy policies and use plain language to explain their data practices. Providing summaries or FAQs can also help users better understand the key points of the policy.

Consent Fatigue: Consent fatigue refers to the phenomenon where users become overwhelmed by the sheer volume of consent requests they receive from various online services. This can lead to users agreeing to terms without fully understanding or considering the implications. To mitigate consent fatigue, organizations should streamline their consent processes and only request consent when absolutely necessary. They should also provide clear and concise explanations of why consent is needed and how the data will be used.

Lack of Transparency: Some organizations may not provide clear information about their data collection and processing practices, making it difficult for users to make informed decisions about consent. This lack of transparency can erode trust and lead to uninformed consent. Organizations should be transparent about their data practices and clearly communicate to users what data is being collected, how it is being used, and who it is being shared with. Providing this information in a clear and accessible manner can help users make informed decisions about their data.

Limited Control: Despite privacy settings that allow users to control their data, users may still have limited control over how their data is collected, used, and shared, especially when it comes to third-party data sharing and advertising. Organizations should give users greater control over their data by providing granular privacy settings that allow them to choose what data is collected and how it is used. Providing opt-out options for certain data processing activities can also give users more control over their data.

Cross-Platform Tracking: Users are often tracked across multiple platforms and devices, making it challenging for them to understand and control the extent of data collection and tracking. This cross-platform tracking can lead to a loss of privacy and a lack of control over one's personal data. To address this challenge, organizations should be transparent about cross platform tracking practices and provide users with options to opt-out of such tracking. Implementing tools such as browser extensions that block tracking cookies can also help users protect their privacy across platforms.

RECENT PRIVACY SCANDALS AND REGULATORY RESPONSES

Overview: The Cambridge Analytica data scandal in 2018 exposed a major breach of privacy involving the unauthorized collection of data from millions of Facebook users worldwide, including in India. The data was used for targeted political advertising by Cambridge Analytica, a political consulting firm.[4]

Background: The scandal originated from a personality quiz app, "This Is Your Digital Life," created by Aleksandr Kogan, a researcher at Cambridge University. The app collected data not only from users who took the quiz but also from their Facebook friends, all without their knowledge or consent. This was possible due to Facebook's data-sharing policies at the time.

Data Harvesting and Usage: Cambridge Analytica contracted Kogan to collect this data and used it to build psychographic profiles of millions of Facebook users. These profiles were then utilized for targeted political advertising, influencing major political events like the 2016 US presidential election and the Brexit referendum.

Impact of the Scandal:

1. **Data Privacy Concerns:** The scandal highlighted significant risks associated with the collection and use of personal data by third parties without proper consent. It underscored the need for stronger data protection regulations and more transparency from tech companies regarding data practices.
2. **Political Manipulation:** The use of psychographic profiling for targeted political advertising raised ethical concerns about the manipulation of voters through personalized messaging, sparking debates on the need for regulations to prevent such practices.
3. **Regulatory Scrutiny:** The scandal led to increased scrutiny from regulatory bodies worldwide. Investigations in the US, UK, and other countries resulted in fines and penalties for Facebook for failing to protect user data.
4. **Reputation Damage:** Facebook’s reputation suffered significantly, with users expressing concerns about privacy and data security on the platform. This resulted in a public backlash and loss of trust.

Response and Fallout: In response to the scandal, Facebook implemented stricter data access policies for third-party developers, requiring more explicit user consent and limiting the amount of data accessible. Facebook also audited apps with extensive data access, suspending those that did not comply with its new policies. The scandal led to the closure of Cambridge Analytica and the suspension of its CEO, Alexander Nix. It also fueled ongoing debates about data privacy and led to calls for stronger regulations to protect user data online. The incident served as a wake-up call regarding the risks associated with the misuse of personal data, prompting changes in data policies and practices among tech companies to restore user trust and enhance privacy protection.

[4] Cambridge Analytica scandal, explained - Google Search, https://www.google.co.in/search?q=Cambridge+Analytica+scandal,+explained&sca_esv=5fbf67e4323cad9e&s (last visited Aug 25, 2024).

SUGGESTIONS FOR ENHANCING USER CONSENT AND DATA PROTECTION

Suggestions for Social Media Platforms:

1. **Transparent Data Practices**: Social media platforms should be transparent about their data collection and processing practices. This includes providing clear and easily accessible information about what data is being collected, how it is being used, and with whom it is being shared. Platforms should also provide users with the ability to access and review the data that has been collected about them.
2. **User-Friendly Consent Mechanisms**: Platforms should implement user-friendly consent mechanisms that allow users to easily understand and control the collection and processing of their data. This includes providing clear explanations of what data is being collected, how it will be used, and giving users the ability to opt-in or opt-out of data collection and processing activities.
3. **Privacy by Design**: Platforms should adopt privacy by design principles, ensuring that privacy is built into their products and services from the outset. This includes implementing data protection measures such as encryption, data minimization, and access controls to protect user data.
4. **Data Minimization**: Platforms should collect only the data that is necessary for their operations and should delete or anonymize data when it is no longer needed. This helps reduce the risk of data breaches and protects user privacy.
5. **Regular Audits**: Platforms should conduct regular audits of their data collection and processing practices to ensure compliance with data protection regulations and to identify and address any potential privacy risks.
6. **User Education**: Platforms should educate users about their data protection rights and how to protect their privacy online. This includes providing information about privacy settings and controls, and offering guidance on how to securely manage their data.
7. **Collaboration with Regulators**: Platforms should collaborate with regulatory authorities to ensure compliance with data protection regulations and to address any concerns or complaints raised by users.

Suggestions for Users:

1. **Be Informed**: Users should educate themselves about data protection laws and regulations and how they apply to the platforms and services they use. This includes understanding what data is being collected about them, how it is being used, and with whom it is being shared. Users should also be aware of their rights under data protection laws, such as the right to access, correct, and delete their personal data.
2. **Be Vigilant**: Users should be vigilant about the data they share online and should regularly review and update their privacy settings. This includes being cautious about the information they share on social media platforms and other online services, and being aware of the privacy implications of their online activities.
3. **Exercise Your Rights**: Users should exercise their data protection rights, such as the right to access, correct, and delete their personal data, as provided for by law. This includes contacting companies or service providers to request access to their data, to correct inaccuracies, or to request deletion of their data. Users should also be aware of how to file complaints with regulatory authorities if they believe their data protection rights have been violated.

CONCLUSION:

The protection of user consent and data on social media platforms is a pressing issue in today's digital landscape. This paper explored the extensive data collected by social media platforms, the challenges in obtaining meaningful user consent, and the significant impact of privacy scandals such as Cambridge Analytica. It highlighted that while there are regulatory advancements, such as the Personal Data Protection Bill, 2019, these efforts must be strengthened and enforced more effectively.

For India, the findings suggest a need for more robust data protection laws and enforcement mechanisms. Social media platforms should improve transparency about their data collection and processing practices and offer clearer, user-friendly consent options. Additionally, increasing public awareness and education about data protection rights will empower users to make informed decisions about their data.

In conclusion, achieving effective user consent and data protection requires ongoing collaboration among policymakers, regulatory bodies, industry stakeholders, and users. This collective effort is crucial to creating a secure and privacy-respecting online environment.

BIBLIOGRAPHY:

ACTS:

1. Information Technology Act,2000

2. Personal Data Protection Act, 2023

WEBSITES:

1. https://www.bbc.com/news/topics/c81zyn0888lt
2. https://www.researchgate.net/publication/301234158_On_Privacy_and_Security_in_Social_Media_A_Comprehensive_StuDy
3. https://www.ijsr.net/archive/v4i12/NOV151933.pdf
4. https://epic.org/issues/consumer-privacy/social-media-privacy/
5. https://www.iacis.org/iis/2021/2_iis_2021_136-149.pdf