AJMR
ISSN (Online) : 2278 - 4853

Asian Journal of Multidimensional Research

Published by :
www.tarj.in

AJMR ISSN (online) : 2278-4853

Editor-in-Chief : Dr. Esha Jain

Impact Factor	:	SJIF 2022= 8.179
Frequency	:	Monthly
Country	:	India
Language	:	English
Start Year	:	2012

Published by : www.tarj.in

Indexed/ Listed at : Ulrich's Periodicals Directory, ProQuest, U.S.A.

E-mail id: tarjjournals@gmail.com

VISION

The vision of the journals is to provide an academic platform to scholars all over the world to publish their novel, original, empirical and high quality research work. It propose to encourage research relating to latest trends and practices in international business, finance, banking, service marketing, human resource management, corporate governance, social responsibility and emerging paradigms in allied areas of management. It intends to reach the researcher's with plethora of knowledge to generate a pool of research content and propose problem solving models to address the current and emerging issues at the national and international level. Further, it aims to share and disseminate the empirical research findings with academia, industry, policy makers, and consultants with an approach to incorporate the research recommendations for the benefit of one and all.

Asian Journal of Multidimensional Research
ISSN: 2278-4853 Vol. 14, Issue 12, December 2025 SJIF 2022 = 8.179
A peer reviewed journal

THE EFFECTIVENESS OF SOCIAL MEDIA PRIVACY SETTINGS IN PROTECTING USERS' PRIVACY: A COMPREHENSIVE STUDY

Manish Tarun*; Gyana Ranjan Panda**

*Research Scholar,
Department of Public Policy, Law and Governance,
Central University of Rajasthan, NH-8, Bandarsindri,
Ajmer, Rajasthan, INDIA
Email Id: manishtarun41291@gmail.com

**Assistant Professor,
Department of Public Policy, Law and Governance,
Central University of Rajasthan, NH-8, Bandarsindri,
Ajmer, Rajasthan, INDIA
Email Id: gyana_pplg@curaj.ac.in

DOI: 10.5958/2278-4853.2025.00036.4

ABSTRACT

This research paper provides a comprehensive examination of the effectiveness of privacy settings on social media platforms in safeguarding user information and privacy rights. Through an extensive literature review and analysis of current scholarly research, this paper investigates the multifaceted challenges surrounding social media privacy protection mechanisms, user behaviour, and the gap between technical capabilities and practical implementation. The study reveals that while privacy settings offer theoretical protection mechanisms, their effectiveness is severely limited by default permissive settings, poor user awareness, complex interface designs, inadequate privacy literacy, and persistent data collection practices by platforms and third parties. The paper analyses how regulatory frameworks, such as GDPR and CCPA, address these concerns while identifying emerging threats, including algorithmic manipulation, facial recognition technologies, deepfakes, and breaches of personal data. Furthermore, this paper examines the "privacy paradox" phenomenon, where users express strong concerns about privacy yet fail to adopt protective measures. Based on a comprehensive analysis of current research findings, the paper recommends a multi-stakeholder approach incorporating privacy-by-design principles, enhanced user education, regulatory enforcement, and platform accountability to improve the effectiveness of social media privacy protection mechanisms.

KEYWORDS: *Social Media Privacy, Privacy Settings Effectiveness, User Privacy Protection, Privacy Literacy, Privacy Concerns, Data Protection Regulations, Privacy Paradox.*

1. INTRODUCTION

The rapid growth of social media platforms such as Facebook, Instagram, Twitter (X), and WhatsApp has transformed global communication and information sharing among billions of users. However, this dramatic expansion has introduced significant challenges related to personal privacy and data protection. Recent statistics show that 76% of Americans mistrust social media

companies, fearing that their personal data may be sold without consent, while 31% have little to no confidence in these companies' ability to safeguard their information (Usercentrics, 2025).

Social media platforms collect vast amounts of user data, including browsing histories, location details, contact lists, biometric identifiers, and behavioural patterns. This information is leveraged for targeted advertising, algorithm-driven content curation, and sharing with third parties. Although privacy settings have been introduced to provide users with control over their personal information, questions remain regarding the effectiveness of these controls. Factors such as poor usability, suboptimal default settings, low user awareness, and ongoing data collection beyond privacy settings limit their ability to protect privacy effectively (Ro, Smith, & Lee, 2024; IEEE Digital Privacy, 2025).

This research critically evaluates the effectiveness of social media privacy settings by examining the interactions among technological capabilities, user behaviour, platform design, regulatory frameworks, and emerging technological threats. It argues that despite seemingly comprehensive privacy options, practical protection is compromised by multiple interconnected challenges, with important implications for user rights, platform accountability, regulatory policy, and the future of digital privacy (User centrics, 2025; IEEE Digital Privacy, 2025).

Understanding these limitations holds critical implications for the protection of user rights, the development of regulatory policy, and holding platforms accountable. As concerns over data breaches escalate and legislation evolves, assessing the practical efficacy of privacy settings is vital for users, developers, policymakers, and advocates committed to enhancing digital privacy (Epic.org, 2025; The Legal School.in, 2025).

2. Background and Context

2.1 The Evolution of Social Media and Privacy Concerns

Social media platforms emerged in the early 2000s as tools primarily designed to facilitate communication and foster connections among users. Platforms such as Friendster, MySpace, LinkedIn, and eventually Facebook revolutionised how individuals interacted online (Landingi, 2025; Online Maryville University, 2024). However, these platforms rapidly evolved beyond simple networking tools into sophisticated data collection and advertising infrastructures. The business models of major social media companies now fundamentally depend on the systematic collection, analysis, and monetisation of user data (Infosys BPM, 2023). This model creates inherent conflicts between platform profitability objectives and user privacy protection concerns.

The Cambridge Analytica scandal, which occurred between 2016 and 2018, represented a watershed moment in public awareness regarding social media privacy vulnerabilities. In this incident, employees and contractors of Cambridge Analytica, a British political consulting firm, accessed private Facebook information belonging to tens of millions of users through a personality quiz application developed by researcher Aleksandr Kogan (Federal Trade Commission, 2022; Schneble et al., 2018). The application harvested data not only from direct users who took the quiz but also from their Facebook friends without explicit consent. Initial reports indicated that approximately 50 million users were affected. However, Facebook later confirmed that the data of up to 87 million users primarily based in the United States had been improperly shared (New York Times, 2018; Wikipedia, 2018). Cambridge Analytica subsequently utilised this data to create detailed psychographic profiles for political targeting purposes during the 2016 U.S. presidential election campaigns.

The Cambridge Analytica scandal exposed fundamental vulnerabilities in social media privacy controls and demonstrated how user data could be systematically exploited despite the theoretical existence of privacy protections. It revealed that Facebook had allowed third-party applications to access not only the data of users who directly engaged with those apps but also the personal information of those users' friends, even when friends had implemented more restrictive privacy settings (Federal Trade Commission, 2019).

The aftermath of the Cambridge Analytica scandal included significant regulatory and financial consequences for Facebook. In July 2019, the Federal Trade Commission voted to impose a $5 billion fine on Facebook, representing the most significant penalty ever assessed by the U.S. government against any company for violating consumers' privacy, nearly 20 times greater than any previous privacy or data security penalty imposed worldwide (Federal Trade Commission, 2019; Reuters, 2019). The ruling specifically cited Facebook's violations of a 2012 FTC consent order, including sharing users' data with third-party applications used by their friends, enabling facial recognition technology by default without proper user consent, and misusing telephone numbers collected for security purposes (such as two-factor authentication) for advertising purposes without disclosure (Federal Trade Commission, 2019; BBC, 2019).

2.2 Privacy Concerns in the Contemporary Digital Landscape

Contemporary research indicates that privacy concerns among social media users have become increasingly pronounced. According to recent survey data, 73% of consumers report heightened concerns about their data privacy compared to previous years, while 64% perceive their data as less secure than in the past (Usercentrics, 2025). Additionally, research indicates that 35% of U.S. adults experience substantial worry about the methods social media platforms employ to collect personal data, with a further 44% expressing some level of concern (Enzuzo, 2024).

These privacy concerns have manifested in observable behavioural shifts among users. Studies reveal that 38% of respondents engage with social media less frequently than previously due to concerns about data privacy, and 36% have discontinued their social media accounts specifically because of privacy-related concerns (Usercentrics, 2025). These statistics underscore that privacy concerns have transcended abstract theoretical discussions to become practical considerations that meaningfully influence user behaviour and platform adoption decisions (Termly.io, 2025).

Furthermore, consumer confidence in social media enterprises has substantially diminished. As of 2024, research indicates that 77% of Americans harbour little to no trust in social media leadership to publicly acknowledge mistakes or assume responsibility for data exploitation, highlighting a crisis of organisational accountability and transparency (Enzuzo, 2024). Most significantly, 89% of Americans express substantial concern about how social media platforms collect personal information about children, reflecting particular apprehension about vulnerable populations (Pew Research Centre, 2023; Usercentrics, 2025). This heightened concern for child privacy is compounded by the fact that 81% of users report having little to no control over the data that social media companies collect and utilise (Usercentrics, 2025).

3. Research Methods

This research employs a comprehensive qualitative literature review and secondary data analysis approach. A descriptive and analytical design was employed to assess the effectiveness of social media privacy settings in safeguarding user privacy. This methodological approach was selected because it enables critical examination of existing scholarly research, regulatory frameworks,

and empirical findings regarding privacy mechanisms and user behaviours. The primary objective of this research was to critically evaluate the effectiveness of privacy settings on social media platforms like Facebook, Instagram, Twitter (X), and WhatsApp in safeguarding user information and privacy rights.

4. Privacy Settings: Definition, Types, and Current Implementations

4.1 Definition and Scope of Privacy Settings

Privacy settings constitute configuration mechanisms established by social media platforms that enable users to manage the visibility of their created content, restrict access to personal information, regulate connections with other platform users, and control how their data is collected and utilised by the platform and external entities. These settings are theoretically intended to actualise the principle of user agency and informed consent within the digital context (SMRI World, 2025).

4.2 Types of Privacy Settings across Major Platforms

Social media platforms employ differentiated approaches to privacy settings that reflect their distinctive business models, demographic user bases, and underlying platform infrastructures (Tech Magnate, 2025).

Facebook constitutes a platform providing detailed privacy settings distributed across multiple organisational categories. Users possess the capacity to regulate post visibility across a spectrum ranging from "Only me", visible exclusively to the account proprietor, to "Public," which renders content visible to all internet users. Intermediate options encompass "Friends," "Friends except," and custom lists configured by individual users. Additional settings allow users to regulate profile discoverability, manage tag approvals, control visibility of contact information, and approve or deny access to third-party applications. However, Facebook's privacy settings remain fragmented across multiple interface tabs, including Privacy, Profile, and Photo Settings, creating a segmented user experience that may contribute to user configuration errors (Social Media Examiner, 2019; SNSin.com, 2024).

Instagram implements relatively simple privacy settings compared to Facebook's architecture. Users can designate their accounts as "Public", permitting anyone to follow and access content, or "Private," which necessitates user approval before prospective followers gain access to their content. Furthermore, Instagram offers settings that allow users to control direct message access and photo tagging functionality. The platform's emphasis on visual content dissemination has resulted in a streamlined privacy architecture compared to Facebook's text-centric social networking model (Tech Magnate, 2025; Webwise, ie, 2018).

Twitter (X) offers two primary privacy configurations: "Public," which makes tweets visible to all internet users and searchable through Twitter's search functionality, and "Protect my Tweets," which restricts tweet visibility to approved followers only. Twitter's structural design as a public conversation forum has historically prioritised content visibility over privacy safeguards, manifesting in the comparative simplicity of privacy controls relative to more closed social network platforms (Troop Messenger, 2024; Webwise, ie, 2018).

5. The Effectiveness Gap: Why Privacy Settings Fail to Protect User Privacy

5.1 Usability and Configuration Errors

Empirical research on privacy settings reveals a substantial discrepancy between users' intended privacy protection and the actual system configurations they implement. A foundational study by Madejski, Johnson, and Bellovin (2012) examining privacy configuration errors in online social networks found that users systematically failed to implement privacy settings aligned with their sharing preferences. In this investigation of 65 participants, every single participant exhibited at least one configuration discrepancy, meaning information was either being shared when the user intended it to remain private or hidden when the user intended to share it. Furthermore, the researchers reported that a substantial majority of participants indicated they either could not or would not address the identified configuration problems (Madejski et al., 2012).

This finding possesses significant implications because it indicates that ineffective privacy protection does not solely result from user indifference or apathy regarding privacy concerns. Instead, the technical and cognitive complexity inherent in privacy control systems creates systematic obstacles to correct implementation. Madejski and colleagues concluded that Facebook's foundational access control mechanism was fundamentally flawed at an architectural level and could not be adequately remedied through marginal enhancements (Madejski et al., 2012).

Comparable patterns emerge in research examining smartphone privacy settings. An investigation of 178 smartphone users revealed that a substantial portion of the population lacks awareness of smartphone privacy and security settings, their default configurations, and has not engaged in configuration modifications beyond the default parameters (Frik et al., 2022). Users encounter particular difficulty when configuring privacy settings that address risks they do not comprehensively understand or perceive as immediate threats (Frik et al., 2022). This phenomenon suggests that usability challenges extend beyond mere interface design to encompass users' cognitive models and their perception of threats.

5.2 Privacy Literacy and User Awareness

A significant obstacle to the effective implementation of privacy settings involves insufficient user awareness and privacy literacy. Privacy literacy constitutes the combination of knowledge, skills, and capability to comprehend privacy mechanisms, identify privacy risks, and deploy appropriate protective measures (UNESCO, 2025). Contemporary research indicates that privacy literacy remains inadequate across substantial proportions of the user population.

A comprehensive analysis of privacy literacy research reveals that adequate privacy protection requires users to possess multiple competency dimensions, including factual knowledge of privacy, privacy-related reflection capacity, privacy and data protection skills, and critical privacy literacy (UNESCO, 2025). Nevertheless, substantial percentages of users lack one or more dimensions. Notably, research indicates that 82.2% of users self-identify as privacy-conscious regarding their browsing history; however, substantial gaps persist in their actual online privacy knowledge (Shrish et al., 2023).

This gap between awareness and knowledge manifests as the "privacy paradox," wherein users articulate substantial privacy concerns yet fail to implement corresponding protective behaviours. Although users express concerns regarding privacy and data management practices, these concerns frequently fail to translate into informed action, such as modifying privacy settings or declining cookie consent requests (Shrish et al., 2023). The principal factors underlying this paradoxical phenomenon include unawareness, limited comprehension of consent

mechanisms and privacy regulations, as well as misconceptions regarding how personal data is processed and safeguarded (Shrish et al., 2023).

5.3 The Privacy Paradox Phenomenon

The privacy paradox exemplifies a central contradiction within contemporary social media privacy research. This phenomenon describes the fundamental inconsistency between users' articulated privacy concerns and their actual privacy-related behaviours. Users overwhelmingly report prioritising privacy and express substantial concerns regarding data collection, yet simultaneously engage in actions that expose their personal information to collection and dissemination mechanisms (Taddicken, 2014).

Contemporary research has identified three principal mechanisms explaining this apparent contradiction (Data Guard, 2025) -

First, personalisation benefits outweigh abstract privacy concerns. Personal data sharing constitutes the primary mechanism enabling the hyper-personalised experiences that drive social media engagement (Momento Science, 2024). In practical terms, users rationally prioritise the immediate benefits and convenience of personalised content over abstract privacy protections (Data Guard, 2025).

Second, users often lack a comprehensive understanding of specific data policies and practices. Privacy policies are characteristically complex, extensive, and employ technical and legal terminology that exceeds the comprehension capacity of average users. This complexity creates formidable barriers to informed consent and understanding of privacy risks (Data Guard, 2025; Daily Economy, 2022).

Third, ubiquitous reports of data breaches establish perceptions of inevitable privacy compromise. Frequent media coverage of security incidents and data breaches creates psychological patterns wherein users perceive privacy protection as futile or impossible (Data Guard, 2025). Users may cognitively process repeated breach reports as evidence that their data has already been compromised or sold, which substantially reduces their motivation to engage in protective practices (Daily Economy, 2022). This "privacy cynicism" represents a rational, if regrettable, psychological adaptation to systemic privacy failures.

5.4 Data Collection Beyond Privacy Settings: The Hidden Data Economy

A fundamental limitation of privacy settings involves their inability to regulate data collection and utilisation occurring beyond the scope of user-visible privacy controls. Social media platforms engage in comprehensive data collection extending beyond user-generated content to encompass metadata, behavioural tracking, and third-party data integration (IEEE Digital Privacy, 2025).

Research on third-party data collection demonstrates that social media platforms systematically utilise data from external sources and partner organisations, which platforms subsequently integrate into algorithmic systems to enable more precise targeting of advertisements. Notably, Facebook and other Meta platforms utilise third-party data to create "lookalike audiences," enabling advertisers to identify and target users exhibiting similar interests and behavioural patterns to existing customer bases (Semeradova & Weinlich, 2019; Oxford Academic, 2025).

Algorithmic profiling and targeted advertising constitute supplementary mechanisms through which privacy protection demonstrates limited practical effectiveness. Personalised marketing

utilising artificial intelligence-powered algorithms on social media platforms has introduced substantial privacy challenges, prompting users to adopt diverse privacy management strategies (Oxford Academic, 2025). The algorithms underpinning social media platforms systematically capture and analyse every user interaction, encompassing content clicked, duration of content viewing, search queries, and metadata to construct comprehensive behavioural profiles for targeted advertising purposes (Oxford Academic, 2025; Transcend, 2023).

5.5 Visibility and Spread of Shared Content

A distinct but related limitation of privacy settings is the inability to control content dissemination once it has been shared with a restricted audience. When users share content through privacy settings configured for specific recipients, those recipients may subsequently repost or share such content to substantially broader audiences beyond the original poster's control. This mechanism generates a significant proportion of social media privacy violations (Tech Target, 2024).

6. Technical and Policy Challenges

6.1 Complexity of Privacy Policies

Social media platform privacy policies constitute extraordinarily lengthy and technologically sophisticated documents. An empirical analysis of 70 digital services found that Facebook and Twitter had the most extensive privacy policies and terms of service among social media platforms, with Twitter's combined policy materials requiring approximately 6.7 hours to read and Facebook's requiring approximately 4 hours (Biggest Lie Online, 2022).

These policies frequently incorporate language authorising expansive data uses, including "targeted advertising," "algorithm optimisation," "third-party sharing," and "security purposes" categories sufficiently broad as to permit nearly any application of user data. Users who configure privacy settings to restrict the visibility of their posts may remain unaware that platforms retain the legal authority to use data regarding their behaviour, interests, and demographics for advertising and algorithmic purposes, independent of their content visibility configurations (Böyük, 2025; Mhaidli et al., 2023).

A privacy policy analysis reveals substantial variations in how different platforms structure their data collection, processing, and dissemination practices. A comparative analysis of privacy policies across Facebook, Instagram, X (Twitter), and WhatsApp reveals significant divergence in platform approaches to user data. However, all major platforms maintain policies permitting extensive data collection and utilisation aligned with the platform's commercial purposes (Böyük, 2025).

6.2 Regulatory Frameworks and Their Limitations

The two most significant regulatory frameworks addressing social media privacy, the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), represent substantial regulatory efforts aimed at enhancing privacy protection. Nevertheless, these frameworks exhibit inherent limitations in ensuring practical privacy protection (WePub, 2025).

6.3 GDPR Implementation and Challenges

The GDPR, implemented in May 2018, established rigorous data protection requirements throughout the European Union. The regulation granted individuals comprehensive rights, including access to their data, the right to rectification, the right to erasure (also known as the "right to be forgotten"), and the right to data portability. The GDPR empowers supervisory authorities to impose penalties of up to €20 million or 4% of the company's annual global turnover; whichever is a greater, establishing substantial financial incentive for compliance (Exabeam, 2025; ProCain Consulting, 2025).

However, GDPR enforcement encounters substantial practical obstacles. The regulation defines personal data expansively to encompass any information that potentially identifies an individual, including both direct identifiers, such as names, and indirect identifiers, such as Internet Protocol addresses. Despite this broad definitional scope, social media platforms have demonstrated a remarkable capacity to maintain technical GDPR compliance while continuing to conduct comprehensive data collection and utilisation practices that serve platform commercial objectives. In numerous instances, platforms have modified their privacy policies to comply with GDPR requirements while maintaining their foundational business model, which is centred on data exploitation (WePub, 2025).

Key GDPR compliance challenges include data mapping and inventory requirements, establishing valid legal processing bases, managing subject access requests, implementing security safeguards, navigating cross-border data transfer restrictions, ensuring third-party vendor compliance, maintaining employee awareness, and sustaining documentation and record-keeping practices (Eurofast, 2025; Neeyamo, 2024). Furthermore, ambiguities persist within the GDPR language. Terms including "undue delay," "likelihood of (high) risk," and "disproportionate effort" remain undefined, necessitating subsequent judicial or regulatory clarification (Thomson Reuters, 2025). The regulation similarly fails to specify what constitutes "reasonable" data protection levels, affording regulators substantial interpretive flexibility in assessing penalties for breaches and non-compliance (Thomson Reuters, 2025).

6.4 CCPA Implementation and Differences from GDPR

The California Consumer Privacy Act, effective January 1, 2020, represents the United States' inaugural comprehensive privacy legislation. The CCPA grants California residents rights, including the right to know about collected personal data, the ability to request data deletion, opt-out mechanisms for data sales and sharing, and non-discrimination protections contingent upon their privacy choices (Thomson Reuters, 2025; Scytale, 2025). The CCPA encompasses broader definitions of personal data than preceding privacy frameworks, including conventional personally identifiable information, as well as browsing history, purchasing patterns, and biometric identifiers.

However, the CCPA's enforcement mechanisms demonstrate a substantially more limited scope than the GDPR provisions. The law establishes penalties of up to $7,500 for intentional violations and $2,500 for unintentional violations, which are substantially lower than the GDPR penalties (Exabeam, 2025; Thomson Reuters, 2025). Furthermore, CCPA applicability is restricted to for-profit businesses conducting California operations that satisfy specified criteria regarding annual revenue or data processing volume, resulting in narrower applicability than the GDPR's global reach (ProCain Consulting, 2025). CCPA specifies no explicit security requirements but holds businesses accountable for implementing security practices, providing less prescriptive guidance than GDPR's detailed security mandates (Exabeam, 2025).

The comparative analysis reveals that the GDPR, characterised by a broader jurisdiction, rigorous enforcement mechanisms, and substantial financial penalties, establishes a more comprehensive and proactive data protection framework relative to the CCPA, which represents a more localised and reactive approach (WePub, 2025). The GDPR mandates supervisory authority investigations and enforcement across European Union member states. In contrast, the CCPA primarily relies on enforcement by the California Attorney General, with consumers retaining private rights of action for specific breach scenarios (Exabeam, 2025).

6.5 Data Breaches and Security Incidents

Despite the existence of privacy settings and regulatory requirements, data breaches continue exposing millions of users' personal information. In April 2021, a significant incident exposed the personal information of 533 million Facebook users, constituting one of the most extensive social media privacy violations (Business Insider, 2021; Forbes, 2021). The leaked dataset encompassed full names, telephone numbers, electronic mail addresses, location information, birthdates, biographical summaries, relationship statuses, and account creation information for users across 106 nations, including 32 million American users, 35 million Italian users, 19.8 million French users, and 11 million British users (Business Insider, 2021; Bitdefender, 2021).

These breaches demonstrate that privacy settings and regulatory compliance provisions are insufficient to prevent security failures from occurring at the platform infrastructure level. Upon unauthorised database access, privacy configurations implemented by individual users become irrelevant to data protection. Research examining data breaches within GDPR and CCPA regulatory frameworks demonstrates that although these regulations mandate breach notification requirements and impose penalties for negligence, they do not fundamentally prevent breaches from occurring (WePub, 2025).

7. Emerging Threats and Advanced Monitoring Techniques

7.1 Algorithmic Manipulation and Targeted Advertising

Modern social media platforms employ advanced artificial intelligence and machine learning algorithms that construct intricate behavioural profiles of users based on every interaction, ranging from likes and comments to viewing and scrolling patterns. These algorithms process massive datasets, leveraging user engagement quality, browsing histories, and even off-platform activity through cross-platform tracking, to predict user preferences and vulnerabilities and facilitate hyper-personalised content delivery (Sprinklr, 2025; Emerge Fibre2Fashion, 2025). The result is an environment in which users are continuously exposed to content tailored for maximal engagement, a process referred to as "algorithmic manipulation." Recent analysis shows these algorithms do not simply display relevant information; they shape user experience by psychologically nudging users toward specific behaviours, opinions, and purchases using reinforcement learning models and real-time engagement feedback signals (Sprinklr, 2025; Emerge Fibre2Fashion, 2025).

7.2 Facial Recognition and Biometric Identification

Another emerging privacy concern stems from the integration of facial recognition and biometric identification technologies within social media platforms. Sophisticated facial recognition software, such as that used by Clearview AI, can identify individuals in photos by comparing them with extensive databases of images scraped from social media without user consent (The Guardian, 2020). These biometric databases now contain tens of billions of images, creating

persistent records of individuals' identities that can be leveraged for surveillance, harassment, or tracking (The Guardian, 2020).

Unlike passwords or usernames, biometric identifiers such as facial features cannot be changed if compromised. The permanent nature of biometric data, coupled with the ability to correlate location or event data from photograph metadata, enables new forms of surveillance and exposes users to identification in sensitive contexts, such as protests or political gatherings (The Guardian, 2020; IEEE Digital Privacy, 2025).

7.3 Deep fakes and Synthetic Media

Recent advancements in artificial intelligence have enabled the creation of deepfakes, synthetic images, audio, or video fabricated to mimic real individuals convincingly. Cybercriminals are increasingly leveraging stolen biometric data from social media to generate deepfake media for fraud, blackmail, or disinformation (IEEE Digital Privacy, 2025). In the United Kingdom, deepfake incidents have reportedly accounted for 32% of security breaches for businesses over the past year (Digital Privacy, 2025).

The combination of facial recognition data with deepfake technology intensifies privacy and security threats. Attackers harvesting facial biometrics or voice samples from social media can create convincing synthetic representations for malicious purposes, with potential ramifications for personal reputation, fraud, and even the manipulation of political processes (IEEE Digital Privacy, 2025).

7.4 Cross-Platform Tracking and Profiling

Contemporary social media companies extend their data collection activities far beyond their own platforms. Through tools such as tracking pixels, cookies, and device fingerprinting, these platforms monitor user behaviours across the broader internet, amassing extensive digital footprints regardless of privacy configurations applied on individual sites (Sprinklr, 2025; Emerge Fibre2Fashion, 2025). This cross-contextual tracking enables the construction of unified behavioural profiles that integrate data on browsing history, location, purchases, and interests, often without explicit user awareness (Sprinklr, 2025).

Research demonstrates that default privacy settings typically do not protect against cross-platform tracking, leaving users' activities visible for aggregation by social networks and their advertising partners. For most users, privacy settings are typically restricted to a single platform's boundaries, offering limited protection from the unified profiles created by internet-scale tracking networks (Sprinklr, 2025; Emerge Fibre2Fashion, 2025).

8. User Behaviour and the Role of Privacy Literacy

8.1 Privacy Literacy as a Determinant of Privacy Behaviour

Empirical research examining the relationship between privacy literacy and privacy-protective behaviour demonstrates that elevated privacy literacy significantly predicts implementation of privacy protection strategies. An investigation of Chinese digital natives revealed that both subjective and objective privacy literacy are positively correlated with privacy protection behaviours, although through distinct mechanisms (Ma et al., 2023). Users reporting higher objective privacy literacy, that is, substantive knowledge and understanding of privacy mechanisms, demonstrate a heightened implementation of privacy protection, including restricting access to photographs, posts, and profiles (Ma et al., 2023).

However, privacy literacy demonstrates only modest predictive capacity regarding actual privacy behaviours. While privacy literacy operationalises a statistically significant predictor of privacy protection, the effect size remains moderate; suggesting that literacy alone constitutes an insufficient driver of sustained privacy-protective behaviour (Ma et al., 2023).

8.2 Privacy Skills and Digital Literacy in Adolescents

Research investigating privacy competencies among adolescent populations demonstrates that targeted digital privacy training and media literacy education significantly enhance privacy awareness. Comprehensive survey research indicates that approximately 83% of adolescents aged 11-18 reported knowing how to adjust privacy settings on social media platforms, though approximately 10% acknowledged unfamiliarity with this concept (ySKILLS, 2023). Notably, 78% of surveyed adolescents reported actively using privacy settings on their social media profiles, although one in five had not employed such controls.

However, substantial gaps persist between adolescents' expressed privacy concerns and actual privacy-protective behaviours. Despite articulating privacy concerns, adolescents frequently fail to implement privacy protection strategies proportionate to their stated concerns, manifesting a developmental variant of the privacy paradox phenomenon (Santer et al., 2021).

8.3 Demographic Variations in Privacy Awareness

Research documents substantial demographic variations in privacy literacy and privacy-protective behaviours across age, education, and socioeconomic dimensions. Generally, investigations consistently demonstrate positive correlations between educational attainment and privacy literacy, with individuals possessing higher educational levels exhibiting enhanced privacy awareness and more frequently implementing privacy protections (Alhazmi et al., 2022; Ojala Burman, 2021).

Age is associated with complex relationships to privacy awareness and behaviour. Research on young users aged 15-32 years indicates heightened privacy concerns compared to older populations aged 33 years and beyond (Alhazmi et al., 2022). However, this heightened concern does not consistently translate into correspondingly elevated protective behaviours, suggesting that concern and action remain decoupled. Additionally, some research suggests that information security awareness increases with age in certain contexts, although this relationship exhibits heterogeneity across populations (Ojala Burman, 2021).

Gender differences in privacy behaviour have been identified, though these patterns remain contested and multidimensional. Research on gender differences in information security awareness has found that women tend to demonstrate higher scores on information security awareness measurements in some studies, although the findings remain inconsistent (Ojala Burman, 2021).

Socioeconomic status similarly influences privacy behaviour. Research examining correlations between socioeconomic status and privacy incidents revealed that individuals from lower socioeconomic contexts reported higher frequencies of self-reported data breaches and privacy incidents, potentially reflecting reduced access to privacy education resources and protective technologies (Alhazmi et al., 2022).

9. Platform-Specific Analysis

9.1 Facebook Privacy Features and Vulnerabilities

Facebook represents the most extensively investigated social media platform concerning privacy effectiveness, likely reflecting its market dominance and historical centrality in privacy controversies. The platform provides relatively granular privacy settings compared to alternative platforms, encompassing detailed audience selection mechanisms, custom friend lists, profile privacy options, and application access controls (Lowens et al., 2025).

However, Facebook's historical record of privacy violations proves extensive. The Cambridge Analytica scandal highlighted how third-party applications could harvest Facebook user data at scale without adequate safeguards on the platform. Subsequent investigations revealed that Facebook continuously facilitates data collection through third-party pixels embedded on external websites, maintains comprehensive tracking through cookie identifiers, and historically enabled facial recognition by default on user-uploaded photographs (Kaspersky, 2025).

9.2 Instagram Privacy Characteristics

Instagram employs a relatively simplified privacy architecture compared to Facebook, reflecting its emphasis on visual content and concentration of younger users. The platform's binary public/private account settings, which permit public profiles visible to all users or private profiles requiring approval before followers access content, are conceptually simpler than Facebook's granular options, potentially reducing configuration errors among non-technical users (Safer Internet, 2021).

However, Instagram's default configuration establishes public account visibility, mandating active user intervention to restrict access. Research indicates Instagram ranks among platforms offering the fewest privacy options and employing the worst default settings overall (Kaspersky, 2025). The platform's structural emphasis on visibility and engagement metrics, including "likes," "follows," and "shares", creates inherent incentive structures toward public account configurations that maximise content visibility (ConsumerReports, 2018).

9.3 Twitter/X Privacy Features

Twitter's foundational architecture as a public conversation platform has significantly constrained its development of privacy features. The platform offers two primary privacy configurations: "Public" tweets, visible to all internet users and discoverable through Twitter's search functionality, and "Protect my Tweets", which restricts visibility to approved followers exclusively (Privacy International, 2025; Comparitech, 2025). Twitter provides minimal capacity to restrict visibility to specific audience segments or to comprehensively control platform data collection beyond tweet protection (Comparitech, 2025).

Contemporary research indicates that Twitter ranks among the weakest platforms in terms of privacy options and default settings (Kaspersky, 2025). The platform's historical business model has prioritised content visibility and public discourse over individual user privacy controls, creating fundamental architectural constraints to enhanced privacy protection.

By default, X collects extensive user behavioural data, including tweets, tweet interactions, link clicks, location information, device characteristics, and third-party analytics from websites utilising Twitter integration. The platform constructs user profiles enabling targeted advertising and algorithmic content delivery. While X provides options to adjust ad personalisation and manage data sharing with business partners, these settings require user knowledge and proactive engagement (Comparitech, 2025; Privacy International, 2025).

10. Recommendations for Improving Privacy Protection Effectiveness

10.1 Privacy by Design Approach

The most fundamental recommendation involves integrating privacy protections into platform development during initial design phases rather than implementing privacy features as supplementary components. Privacy by Design (PbD), a framework developed by Dr. Ann Cavoukian and formalised through collaborative work with the Information and Privacy Commissioner of Ontario and Dutch authorities, encompasses seven foundational principles: proactive threat identification; privacy as default configuration; full design integration; positive-sum functionality without privacy-security trade-offs; end-to-end security; visibility and transparency; and respect for user privacy (Cavoukian, 1995; CES Privacy, 2025).

10.2 Enhanced Default Settings and Simplification

Substantial improvements in the effectiveness of privacy protection could be achieved through the reformulation of default privacy settings toward more restrictive configurations. Establishing privacy as the default, encompassing restricted content visibility to approved followers and limiting third-party data sharing, would eliminate requirements for users to actively implement privacy configurations (ShareID, 2024).

Additionally, simplified privacy settings interface architecture would substantially mitigate usability barriers and configuration errors. Rather than fragmenting privacy settings across multiple tabs and menu locations, a current practice that contributes to user misconfiguration, consolidating settings into a single, intuitive interface would substantially facilitate correct configuration (Lowens et al., 2025). Platform designers should employ human-centred design methodologies informed by usability research to construct privacy setting interfaces enabling correct configuration across diverse technical competency levels (Cavoukian, 1995; CES Privacy, 2025).

10.3 User Education and Privacy Literacy Enhancement

Meaningful improvements in the effectiveness of privacy protection require comprehensive user education that addresses privacy risks, privacy mechanisms, and privacy-protective practices. Educational initiatives should encompass diverse demographic groups utilising multiple delivery modalities, including in-application instruction, external educational content, school curricula, and public awareness campaigns (Ma et al., 2023).

10.4 Regulatory Enhancement and Enforcement

Although GDPR and CCPA represent substantial regulatory advancements, both frameworks necessitate enhancements to operationalise meaningful privacy protection. Regulatory improvements should encompass heightened penalties for violations, particularly for intentional ones, intensified enforcement mechanisms, and explicit specifications regarding privacy setting defaults and algorithmic transparency requirements (WePub, 2025).

Additionally, regulatory frameworks should mandate platform accountability for third-party data access and require platforms to conduct periodic audits evaluating the effectiveness of privacy settings to identify and remediate configuration failures at scale. Regulatory requirements should establish that the effectiveness of privacy settings will be measured not by the mere existence of privacy controls, but by the actual user protection achieved through these controls (ProCain Consulting, 2025).

10.5 Technical Solutions and Privacy-Enhancing Technologies

Technical innovations in privacy-enhancing technologies (PETs) could significantly enhance the effectiveness of privacy protection. Key innovations include:

Consent Management Platforms (CMPs) constitute standardised systems for managing user consent across platforms and third parties, enabling users to exercise privacy preferences at scale. Contemporary CMPs incorporate AI-powered consent management and integration with privacy-preserving analytics platforms (Didomi, 2025; Cookie Script, 2025).

Privacy-Preserving Analytics enable platforms to derive behavioural insights without compromising privacy through anonymisation, data aggregation, and differential privacy techniques (Tech GDPR, 2025; Cookie Script, 2025). Differential privacy specifically operates by introducing mathematical randomness into data analysis, rendering individual identification substantially more difficult while permitting population-level statistical analysis (Didomi, 2025).

End-to-end encryption implements encryption mechanisms that prevent even platform operators from accessing user communications and content, as employed by Signal and WhatsApp (Tech GDPR, 2025).

10.6 Platform Transparency and Algorithmic Accountability

Meaningful privacy protection necessitates that social media platforms furnish transparent information regarding user data collection, processing, and utilisation. Existing privacy policies remain insufficiently transparent regarding algorithmic decision-making, specifics of third-party data sharing, and the extent of comprehensive data collection (CES Privacy, 2025).

Platforms should be required to provide clear and comprehensible explanations of their data practices, enabling users to understand how their data affects algorithmic recommendations and targeted advertising. Additionally, platforms should facilitate meaningful user control over algorithmic curation, permitting users to understand content recommendation rationales and to reject algorithmic recommendations in favour of chronological or non-algorithmically curated content alternatives (Postiz, 2025).

10.7 Alternative Platform Models

The fundamental limitations of privacy protection within existing social media business models suggest that alternative platform architectures may prove necessary to ensure genuine privacy protection. Emerging platforms exemplify alternative models, including:

Decentralised platforms, such as Bluesky, employ decentralised protocols, distributing data and processing across independent servers rather than centralising data on a single platform server. Bluesky's AT Protocol (Authenticated Transfer Protocol) emphasises data portability and user autonomy, enabling users to migrate accounts across servers without losing followers (OKX, 2025; Postiz, 2025; IFTTT, 2025).

Federated Platforms, such as Mastodon, implement federation models wherein independent instances operate separately while maintaining interoperability, allowing users to select instances with privacy policies that align with their preferences. Mastodon is fully decentralised, permitting anyone to establish an instance and establish distinct governance rules (OKX, 2025; Postiz, 2025; IFTTT, 2025). Mastodon offers chronological timelines that are free from

algorithmic manipulation, ensuring users encounter posts in the order they were published, which fosters more authentic engagement (Postiz, 2025).

11. Discussion and Analysis

The evidence examined throughout this research demonstrates that, despite their theoretical protective promises, social media privacy settings remain substantially ineffective in practice at protecting user privacy. This ineffectiveness stems not from singular failure mechanisms but rather from multiple interconnected factors operating at technical, behavioural, regulatory, and systemic levels.

At the technical level, privacy settings fail due to complexity, poor usability, inadequate defaults, and fundamental inability to control data collection and utilisation occurring beyond user-visible settings (Lowens et al., 2025). Users who make genuine efforts to protect their privacy frequently misconfigure settings, resulting in data sharing that exceeds their intended audience scope (Madejski et al., 2012).

At the behavioral level, privacy literacy remains inadequate across substantial user populations, preventing the comprehension of privacy risks or the correct implementation of available protective measures (Ma et al., 2023). The privacy paradox phenomenon reveals that privacy concerns alone are insufficient for motivating privacy-protective behaviour when users perceive the benefits from data sharing and personalisation as outweighing the privacy risks (Data Guard, 2025).

At the regulatory level, existing frameworks, including GDPR and CCPA, while representing progress, remain insufficient to ensure meaningful privacy protection (WePub, 2025). These frameworks permit substantial data collection and utilisation for platform purposes while providing users with limited meaningful control (ProCain Consulting, 2025).

At the systemic level, the business models of major social media platforms fundamentally depend on exploiting user data for advertising and algorithmic purposes. Privacy protection remains fundamentally misaligned with these business models, creating essential conflicts between platform interests and user privacy protection (Postiz, 2025).

The emerging technological threats, including algorithmic profiling, facial recognition, deepfakes, and cross-platform tracking, demonstrate that privacy risks escalate beyond the capacity of privacy settings to address. Future privacy protection mechanisms must address these increasingly sophisticated threats (IEEE Digital Privacy, 2025).

12. CONCLUSION

This comprehensive research paper has examined the effectiveness of social media privacy settings in protecting user privacy. The evidence unequivocally demonstrates that while privacy settings offer theoretical protective mechanisms, their practical effectiveness remains substantially constrained by technical complexity, poor usability, inadequate user awareness and literacy, permissive default configurations, and the ongoing exploitation of user data through mechanisms operating beyond the scope of privacy settings.

The Cambridge Analytica scandal, multiple substantial data breaches, regulatory penalties, and proliferating privacy threats underscore urgent requirements for enhanced privacy protection mechanisms. Current research indicates that 38% of users now use social media less frequently due to privacy concerns, and 36% have entirely discontinued their social media accounts for

similar reasons (Usercentrics, 2025). These behavioural changes demonstrate that users recognise inadequacy in current privacy protection mechanisms.

Meaningful improvement in the effectiveness of privacy protection requires coordinated action across multiple domains. Technical solutions must address usability barriers and default setting permissiveness. Regulatory frameworks must be strengthened to enforce greater platform accountability and higher penalties for violations. User education must enhance privacy literacy across diverse demographic segments. Platform transparency must enable users to comprehend data practices and exercise meaningful control. Emerging alternative platform models may prove necessary to ensure privacy protection becomes structurally embedded in platform design rather than contingent upon user configuration (CES Privacy, 2025).

The future of social media privacy will likely be shaped by three interrelated developments: escalating demand for privacy protections from increasingly aware users and regulatory bodies; technological advances enabling more sophisticated privacy-enhancing solutions and alternative platform architectures; and business model evolution toward approaches enabling platform functionality and personalisation without requiring user data exploitation (Postiz, 2025).

Privacy constitutes not merely a technical problem to be resolved through improved settings or encryption protocols. Instead, privacy protection requires fundamental reconceptualisation of social media platform purposes, business models, and platform-user relationships. As long as social media platforms priorities primary business objectives centered on user data collection and exploitation for advertising purposes, privacy settings will remain inadequate to protect user privacy (Pro Cain Consulting, 2025). Genuine privacy protection will necessitate either a transformation of platform business models or the development of alternative platforms designed with privacy as a foundational principle, rather than an afterthought (Postiz, 2025; IFTTT, 2025).

REFERENCES

1. Alhazmi, H., Alhazmi, T., & Matengu, K. (2022). How do socio-demographic patterns define digital privacy divide? ArXiv Preprint arXiv: 2203.16577. https://doi.org/10.48550/arXiv.2203.16577
2. ArXiv. (2024, December 10). Large-scale audit of algorithmic biases and LLM profiling: Reconstructing demographics from Facebook ads. Retrieved from arxiv.org
3. BBC. (2019, July 23). Facebook to pay record $5bn to settle privacy concerns. BBC News. https://www.bbc.com/news/technology-48878452
4. Biggest Lie Online. (2022, December 3). A policy length analysis for 70 digital services. https://biggestlieonline.com
5. Bit defender. (2021, April 4). Phone numbers and associated profile info of 533 million Facebook users leaked online. https://www.bitdefender.com
6. Böyük, M. (2025). Privacy policies of social media platforms. Retrieved from dergipark.org.tr
7. Business Insider. (2021, April 2). Stolen data of 533 million Facebook users leaked online. https://www.businessinsider.com
8. Carbide Security. (2023, June 19). The seven principles of privacy by design. https://carbidesecure.com

9. Cavoukian, A. (1995). Privacy by design: The foundational principles [Joint report]. Information and Privacy Commissioner of Ontario, Dutch Data Protection Authority, and Netherlands Organisation for Applied Scientific Research.

10. CES Privacy. (2025, September 15). Privacy by design. https://cesprivacy.org

11. Clarip. (2021, July 31). Privacy by default: The practical application of simplified privacy. https://clarip.com

12. CNET. (2019, December 20). Default settings for privacy -- we need to talk. https://cnet.com

13. Comparitech. (2025, June 21). Twitter privacy settings: A guide to secure your X account. https://comparitech.com

14. Consumer Reports. (2018, November 1). Instagram privacy settings you should change right now. https://consumerreports.org

15. Cookie First. (2023, January 11). What is privacy by default? https://cookiefirst.com

16. Cookie Script. (2025, June 22). Privacy-enhancing technologies & the future of consent. https://cookie-script.com

17. Daily Economy. (2022, October 27). Privacy in social media: The paradox does not exist. Retrieved from thedailyeconomy.org

18. Data Guard. (2025, January 22). Understanding the privacy paradox: Ethical marketing, privacy concerns and behavior. Retrieved from dataguard.com

19. Data Guard. (2025, January 22). Understanding the privacy paradox: Ethical marketing, privacy concerns and behavior. https://dataguard.com

20. Didomi. (2025, February 8). Privacy enhancing technologies (PETs): What you need to know. https://didomi.io

21. Digital Privacy. (2025, May 12). Privacy risks and social media. IEEE Digital Privacy. https://digitalprivacy.ieee.org

22. Disaster Recovery Journal. (2025, September 24). Social media privacy ranking 2025. https://drj.com

23. DPO Club. (2025, October 6). TikTok's data privacy troubles in Europe. https://dpoclub.in

24. EM360Tech. (2025, July 16). What is privacy by design and default? An essential guide. https://em360tech.com

25. Emerge Fibre2Fashion. (2025, September 22). How AI algorithms transform social media content discovery. https://emerge.fibre2fashion.com

26. Emplicit. (2025, July 24). 5 TikTok data privacy rules for sellers. https://emplicit.co

27. Enzuzo. (2024, February 7). 79 eye opening data privacy statistics for 2024 (updated!). https://enzuzo.com

28. Eurofast. (2025, January 19). Key compliance challenges of GDPR and strategies to overcome them. https://eurofast.eu

29. Exabeam. (2025, June 26). GDPR vs. CCPA: 3 similarities and 6 differences. https://www.exabeam.com

30. Federal Trade Commission. (2019, July 24). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

31. Federal Trade Commission. (2022, January 26). FTC issues opinion and order against Cambridge Analytica. https://www.ftc.gov/news-events/news/press-releases/2022/01/ftc-issues-opinion-order-against-cambridge-analytica

32. Forbes. (2021, April 3). Personal data of 533 million Facebook users leaks online. https://www.forbes.com

33. Frik, A., Hartzog, W., Mustafaraj, E., & Vitak, J. (2022). Users' expectations about and use of smartphone privacy settings. ACM Transactions on Computing Education, 22(4), Article 62. https://doi.org/10.1145/3528257

34. IEEE Digital Privacy. (2025). Privacy risks and social media. IEEE Digital Privacy. https://digitalprivacy.ieee.org

35. IEEE Digital Privacy. (2025). Privacy risks and social media. IEEE Digital Privacy. Retrieved from digitalprivacy.ieee.org

36. IEEE Digital Privacy. (2025). Privacy risks and social media. IEEE Digital Privacy. https://digitalprivacy.ieee.org

37. IFTTT. (2025, March 10). Bluesky vs Mastodon: What are the differences?. https://ifttt.com

38. Infosys BPM. (2023, November 19). Monetize social media with data analytics. https://www.infosysbpm.com/blogs/digital-experience/monetize-social-media-with-data-analytics.html

39. Kaspersky. (2025, October 28). Which social media are the most privacy-oriented in 2025. https://kaspersky.com

40. Kiteworks. (2025, July 30). What is the California Consumer Privacy Act (CCPA)?. https://www.kiteworks.com

41. Landingi. (2025, August 24). Social media marketing history and its revolution over time. https://landingi.com/blog/social-media-marketing-history/

42. Lee, H. (2019). The nonlinear relationship between age and information privacy concerns: Reconsidering the privacy paradox. Computers in Human Behavior, 100, 332-340. https://doi.org/10.1016/j.chb.2019.07.001

43. Lowens, B., Freedman, M., & Shaer, O. (2025). Misalignments and demographic differences in expected and actual privacy settings on Facebook. Proceedings on Privacy Enhancing Technologies, 2025(1), 1-23.

44. Lowens, B., Freedman, M., & Shaer, O. (2025). Misalignments and demographic differences in expected and actual privacy settings on Facebook. Proceedings on Privacy Enhancing Technologies, 2025(1), 1-23.

45. Ma, S., Chen, L., & Wang, X. (2023). Are digital natives overconfident in their privacy literacy? Examining subjective and objective privacy literacy on privacy protection behavior. Frontiers in Psychology, 14, 1164372. https://doi.org/10.3389/fpsyg.2023.1164372

46. Ma, S., Chen, L., & Wang, X. (2023). Are digital natives overconfident in their privacy literacy? Examining subjective and objective privacy literacy on privacy protection behavior. Frontiers in Psychology, 14, 1164372. https://doi.org/10.3389/fpsyg.2023.1164372

47. Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. In Proceedings of the 2012 IEEE International Workshop on Security and Privacy in Social Networks (pp. 1-8). IEEE. https://doi.org/10.1109/IWSPN.2012.6555918

48. Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. In Proceedings of the 2012 IEEE International Workshop on Security and Privacy in Social Networks (pp. 1-8). IEEE.

49. Masur, P. K. (2023). Challenges in studying social media privacy literacy. Research Synthesis Methods, 12(3), 289-301. https://doi.org/10.1002/jrsm.1485

50. Media Laws EU. (2025, June 4). Why TikTok was fined half a billion under the GDPR. https://medialaws.eu

51. Meta. (2025). Meta privacy policy: How Meta collects and uses user data. Retrieved from facebook.com

52. Mhaidli, A., Wüest, K., Held, C., & Schaub, F. (2023). Researchers' experiences in analyzing privacy policies. Privacy Enhancing Technologies Symposium, 1-21.

53. Momento Science. (2024, November 3). Personalization and Gen Z: Why one-size-fits-all does not work. Retrieved from blog.momentscience.com

54. Mozilla Blog. (2019, June 3). When it comes to privacy, default settings matter!. https://blog.mozilla.org

55. Neeyamo. (2024, December 26). Navigating GDPR: Key challenges & compliance strategies. https://www.neeyamo.com

56. New York Times. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

57. Ojala Burman, E. (2021). Impact of demographic factors on information security awareness [Master's thesis]. Diva Portal.

58. OKX. (2025, July 27). Decentralized social media: How Mastodon, Bluesky, and others compare. https://okx.com

59. Online Maryville University. (2024, April 23). The evolution of social media: How did it begin, and where could it go next? https://online.maryville.edu/blog/evolution-social-media/

60. Oxford Academic. (2025, October 7). Latent privacy management profiles on algorithmic social media. Retrieved from academic.oup.com

61. Pew Research Center. (2023, October 17). Key findings about Americans and data privacy. https://pewresearch.org

62. Postiz. (2025, June 2). Mastodon vs Bluesky: Top decentralized social platforms compared. https://postiz.com

63. Privacy Canada (Office of the Privacy Commissioner of Canada). (2025, September 22). Joint investigation of TikTok Pte. Ltd. by the Office of the Privacy Commissioner of Canada and the Commission d'accès à l'information du Québec. https://priv.gc.ca

64. PrivacyInternational. (2025, August 10). Guide on X settings and good practices. https://privacyinternational.org

65. ProCain Consulting. (2025, August 31). Data privacy regulations: GDPR, CCPA & Indian IT Act. https://www.procainconsulting.com

66. ProCain Consulting. (2025, August 31). Data privacy regulations: GDPR, CCPA & Indian IT Act. https://procainconsulting.com

67. Reuters. (2019, July 24). Facebook to pay record $5 billion U.S. fine over privacy. https://www.reuters.com/article/us-facebook-ftc-idUSKCN1UJ1C9

68. Ro, E., Smith, J., & Lee, K. (2024). A survey of social media users' privacy settings and behavior. Regional Online Education Journal, 15(3), 45-60.

69. Safer Internet. (2021, October 20). Privacy settings on Instagram – what do they mean?. https://saferinternet.org.uk

70. Santer, N. D., Buijzen, M., & Valkenburg, P. M. (2021). Early adolescents' perspectives on digital privacy. The Mitre Review, 11(2), 45-78.

71. Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. EMBO Reports, 19(8), e46579. https://doi.org/10.15252/embr.201846579

72. Scytale. (2025, July 23). The CCPA compliance checklist. https://www.scytale.ai

73. SecPod. (2025, March 6). Story of cyberattack – Facebook data leak. https://www.secpod.com

74. Semerádová, T., & Weinlich, P. (2019). Advertising expenditures and its effectiveness in the e-commerce market. In Proceedings of the 20th International Conference on Digital Transformation and Global Society (pp. 450-461).

75. ShareID. (2024, December 9). Privacy by design: Definitions and principles. https://shareid.ai

76. Shrish, S., Priya, K., Garg, S., & Kumari, M. (2023). Exploring privacy perspectives of Indian internet users in relation to cookie banners and privacy regulations. ArXiv Preprint arXiv: 2305.01234.

77. Simplified.com. (2020, October 18). What do you mean by privacy settings on social media?. https://simplified.com

78. SMRI World. (2025). Privacy settings. https://smri.world

79. SNSin.com. (2024, June 26). A guide to social media privacy settings. https://snsin.com

80. SocialMediaExaminer. (2019, January 20). How to check social media privacy settings. https://socialmediaexaminer.com

81. Sprinklr. (2025, July 2). Social media algorithm and how they work in 2025. https://sprinklr.com

82. StoryChief. (2025, September 29). Social media algorithm 2025: How to optimize for all platforms. https://storychief.io

83. Strobes. (2025, March 23). Top data breaches of January 2025. https://www.strobes.co

84. Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, psychological traits, and attitudes on self-disclosure. Journal of Computer-Mediated Communication, 19(2), 248-273. https://doi.org/10.1111/jcc4.12052

85. Tech GDPR. (2025, May 12). How privacy enhancing technologies (PETs) can help organizations. https://techgdpr.com

86. Tech Magnate. (2025, September 2). Instagram vs. Facebook vs. Twitter (X) vs. Snapchat. https://techmagnate.com

87. Tech Target. (2024, October 31). 6 common social media privacy issues. Retrieved from techtarget.com

88. Termly.io. (2025, November 11). 64 alarming data privacy statistics businesses must see. https://termly.io

89. The Guardian. (2020, February 27). Clearview AI: company claims to have scraped 10bn photos for facial recognition database. https://theguardian.com

90. Thomson Reuters. (2025, June 2). Top five concerns with GDPR compliance. https://legal.thomsonreuters.com

91. Thomson Reuters. (2025, November 7). Understanding the California Consumer Privacy Act (CCPA). https://legal.thomsonreuters.com

92. TikTok Support. (2024, December 31). Account privacy settings. https://support.tiktok.com

93. Transcend. (2023, November 30). Examining privacy risks in AI systems. Retrieved from transcend.io

94. Troop Messenger. (2024, October 16). Managing default app and social media settings. https://troopmessenger.com

95. UNESCO. (2025). Survey on privacy in media and information literacy. United Nations Educational, Scientific and Cultural Organization. Retrieved from unesco.org

96. Usercentrics. (2025, June 26). Facebook privacy policy: A complete guide for businesses. Retrieved from usercentrics.com

97. User centrics. (2025, November 10). 150 data privacy statistics for 2025 you need to know about. https://usercentrics.com

98. User centrics. (2025, November 10). 150 data privacy statistics for 2025 you need to know about. https://usercentrics.com

99. Usercentrics. (2025, October 28). 150 data privacy statistics for 2025 you need to know about. https://usercentrics.com

100. VerityAI. (2025). How social media algorithms enable mass cognitive manipulation. https://verityai.co

101. Webwise.ie. (2018, June 11). Protecting your privacy on 9 popular social networks. https://webwise.ie

102. WePub. (2025, January 22). Evaluating the effectiveness of GDPR and CCPA in safeguarding consumer data. https://www.wepub.org

103. WePub. (2025, January 22). Evaluating the effectiveness of GDPR and CCPA in safeguarding consumer data. https://wepub.org

104. Wikipedia. (2011, August 3). Privacy by design. https://en.wikipedia.org/wiki/Privacy_by_design

105. Wikipedia. (2018, March 25). Facebook–Cambridge Analytica data scandal. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

106. Y SKILLS. (2023). Interpersonal and commercial dimensions of privacy literacy. Digital Skills and Online Safety EU Project. https://yskills.eu

Asian Journal of Multidimensional Research
ISSN: 2278-4853 Vol. 14, Issue 12, December 2025 SJIF 2022 = 8.179
A peer reviewed journal

HOW GENERATIONAL CHANGE IS TRANSFORMING MICROFINANCE: THE ROLE OF MILLENNIALS AND GENERATION Z IN INCLUSIVE AND SUSTAINABLE DEVELOPMENT

Vishnu Datta*; Dr.Alok Singh**

*Research Scholar in Commerce,
Shyama Prasad Mukherjee Government Degree College,
University of Allahabad, Prayagraj, INDIA
Email Id: vishnudatta88363@gmail.com

**Assistant Professor of Commerce,
Shyama Prasad Mukherjee Government Degree College,
University of Allahabad, Prayagraj, INDIA
Email Id: draloksingh@outlook.com

DOI: 10.5958/2278-4853.2025.00037.0

ABSTRACT

Microfinance has emerged as a key instrument for promoting financial inclusion and poverty reduction, yet its evolution is increasingly influenced by generational change and shifting development priorities. With a focus on millennial-led innovation and the growing importance of Generation Z, this study attempts to investigate how generational changes impact microfinance as a tool for equitable and sustainable development. Based on a thorough analysis of excellent secondary literature, the study uses an exploratory and theoretical research approach. A values–innovation–inclusion framework that describes the connection between generational values, innovation orientation, and inclusive financial results is created using an interpretative analytical approach. According to the report, millennials have greatly changed microfinance through customer-centric models, digital platforms, and sustainability-focused practices, increasing access and enhancing service relevance for underprivileged populations. The results also indicate that Generation Z will probably have an impact on future microfinance models through ecosystem-based, green, and digital-first strategies that connect finance with sustainable livelihoods and skill development. By emphasising the necessity of creating adaptable, technologically advanced, and sustainability-focused financial models that are in line with changing generational expectations and long-term development objectives, the study presents future implications for policymakers and microfinance organisations.

KEYWORDS: *Microfinance, Generational Shifts, Millennials, Generation Z, Financial Inclusion, Sustainable Development.*

INTRODUCTION

Microfinance has become an important development instrument for addressing financial exclusion and reducing poverty, particularly in developing economies. Microfinance gives low-income people access to fundamental financial services including credit, savings, insurance, and payments, allowing them to engage in economic activities that promote income production and

livelihood stability. Its function has evolved over time from microcredit to a more comprehensive framework for financial inclusion that supports development, inclusive growth, and entrepreneurship (Chibba, 2009; Chen et al., 2017). However, social change, technology advancement, and altering development priorities all have an impact on the evolution of microfinance.

One key but relatively underexplored factor shaping this evolution is generational change.According to the generational cohort hypothesis, common socioeconomic and technical experiences help different generations form unique values, attitudes, and behavioural patterns. These variations have an impact on the development, uptake, and application of financial services. With significant ramifications for the provision of microfinance, generational changes have prompted a shift away from conventional, institution-centered financial models and towards more adaptable, technology-enabled, and user-focused strategies in recent decades (Tulgan, 2004).

By incorporating digital platforms, fintech solutions, and impact-oriented business models, millennials have significantly contributed to the transformation of microfinance. Microfinance is becoming a tool for inclusive financial development rather than only a means of reducing poverty thanks to its focus on innovation, transparency, and social purpose (Chen et al., 2017; Chatterjee, 2020). In the future, it is anticipated that Generation Z will have a greater impact on microfinance due to their increased interest in ethical and sustainable business practices, desire for technology-based financial participation, and digital literacy. Research indicates that Gen Z is highly responsive to digital financial innovation and education, underscoring its potential contribution to future poverty alleviation and sustainable economic change (Sconti, 2022).In this context, the study develops a conceptual framework that integrates microfinance, generational, and sustainability perspectives to explain how generational shifts shape inclusive finance and development outcomes.

Review of Literature

Bruce Tulgan (2004) investigated the emerging generational change in the workforce in order to comprehend shifting employee values and employer-employee relationships. The study found a shift towards transactional employment arrangements using a ten-year qualitative approach that included surveys, organisational studies, and interviews. The study comes to the conclusion that workplace standards have changed due to generational shifts, with an emphasis on self-managed careers, flexibility, and short-term rewards.

Chibba (2009) examines how financial inclusion contributes to poverty reduction and the achievement of Millennium Development Goals.By identifying important pillars and models, the study seeks to understand the relationship between financial inclusion and poverty. The study draws the conclusion that expanding inclusive financial systems is crucial for sustainable development and successful poverty reduction through field research, secondary literature, and international case analysis.

Nga, Yong, and Sellappan (2010) investigated teens' general and financial product awareness in order to determine the impact of education and demographics. The study concluded that organised financial education is crucial for enhancing young people's financial decision-making after using a survey of 280 Malaysian students and multivariate analysis to find that education level and field of study significantly affect financial awareness.

Chen, Chang, and Bruton (2017) looked at the state and prospects of microfinance research in order to evaluate its contribution to the growth of entrepreneurship and the alleviation of poverty. The authors came to the conclusion that microfinance outcomes are inconsistent and context-dependent after conducting a thorough analysis of empirical and theoretical research published in prestigious publications. This underscores the need for targeted, comparative, and theory-driven future research.

Abu Daqar, Arqawi, and Abu Karsh (2020) examined Millennials' and Generation Z's perceptions of fintech services with the objective of understanding their financial behavior and adoption intentions.The study discovered that trust, usability, and real-time services have a significant impact on adoption in the Palestinian setting using a questionnaire-based survey and descriptive analysis. It comes to the conclusion that fintech enhances banking, and banks are urged to digitise services in order to cater to the needs of different generations.

Kulmie et al. (2023) examined the role of entrepreneurship training in job creation and youth empowerment.The goal of the study was to determine how structured training improves young people's employability and financial independence. The writers discovered that entrepreneurship training improves abilities, self-assurance, and revenue prospects by a thorough analysis of secondary research. The study came to the conclusion that incorporating entrepreneurship training into national and educational policy is essential for empowering young people and reducing poverty.

Yap, Lee, and Liew (2023) examined how financial inclusion contributes to achieving finance related Sustainable Development Goals.Using a cross-country panel regression approach, the study sought to evaluate the consequences of the SDGs individually and collectively for 76 nations between 2017 and 2020. The results show that financial inclusion greatly promotes economic growth, gender equality, and the decrease of hunger, all of which enhance overall sustainable development outcomes.

Objectives

- To develop a conceptual framework explaining how generational shifts influence the evolution of microfinance as a tool for inclusive financial development.
- To integrate microfinance, generational, and sustainability theories in order to explain millennial-driven innovations in financial inclusion.
- To conceptualize the prospective role of Generation Z in poverty reduction and sustainable economic transformation through future-oriented microfinance models.

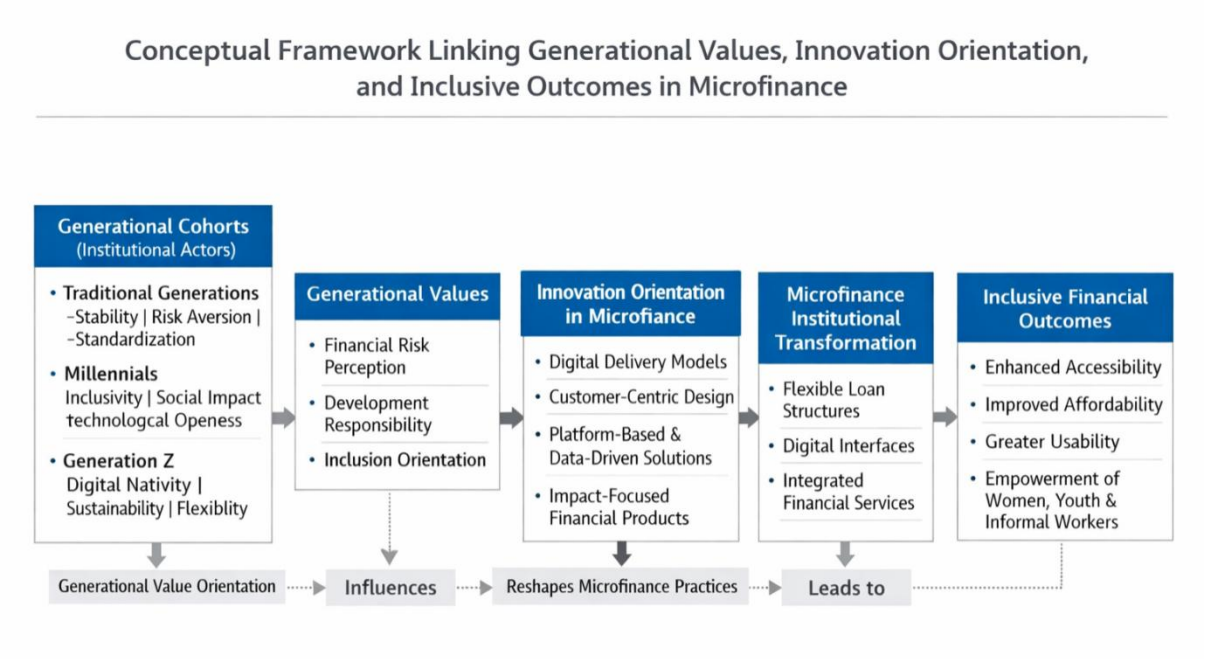
Research Methodology

This study adopts an **exploratory research design** and is **theoretical in nature**. It relies exclusively on **secondary data** drawn from high quality peer-reviewed research papers, journals, articles. A **systematic and thematic literature review** informs the **analytical framework**, which applies interpretative analysis to develop a **values-innovation-inclusion framework**. A **scenario-based approach** is further employed to examine the prospective role of Generation Z in future-oriented microfinance models.

Discussion and Analysis

1. Conceptual Framework of Generational Shifts in Microfinance Development:

Microfinance has evolved as a key instrument for inclusive financial development, shaped significantly by changing generational values and approaches.Microfinance's goals, methods of distribution, and use of technology have all changed as a result of generational upheavals, altering how it addresses new socioeconomic and developmental demands.



Source: *Compiled by Author*

- **Conceptualization of Generational Cohorts in Microfinance**

According to the suggested concept, generational cohorts are seen as socially formed groupings that are influenced by common value systems, technological exposure, and economic circumstances. Traditional generations, millennials, and Generation Z are viewed in microfinance as institutional actors whose shared values impact organisational priorities and financial decisions, allowing for a socio-institutional analysis as opposed to only a financial one.

- **Generational Values as Foundational Constructs**

According to the framework, the fundamental force behind the evolution of microfinance is generational values. Stability, risk aversion, and standardised financial processes are valued by traditional generations. While Generation Z exhibits digital nativity, sustainability consciousness, and adaptability, Millennials prioritise inclusivity, social effect, and technological adoption. These value orientations collectively influence how microfinance systems see risk, development responsibility, and financial inclusion.

- **Generational Influence on Innovation Orientation in Microfinance**

It is believed that innovation orientation acts as a mediator between microfinance methods and generational values. Innovation adoption across cohorts is influenced by differences in problem-

solving techniques and technical familiarity. While Generation Z pushes platform-based, data-driven, and impact-oriented solutions, millennials support customer-centric and digital models, while traditional groups favour procedural stability. These generational beliefs have the potential to revolutionise microfinance operations.

- **Microfinance Reshaping Through Generationally Driven Innovation**

The framework demonstrates how institutional aspects of microfinance, including client involvement, delivery methods, and product design, are altered by generationally driven innovation. Flexible loan arrangements, digital interfaces, and bundled services are some of the results that show how transactional lending has given way to a more responsive and adaptable system influenced by changing generational preferences.

Linking Innovation to Inclusive Financial Outcomes

- Inclusive finance is conceptualized as the outcome constructs in the framework. The improved use, affordability, and accessibility of financial services provides an explanation for the relationship between innovation and inclusiveness. Innovations impacted by generations lower obstacles to entrance, increase the relevance of services, and bolster client empowerment. Microfinance's role in inclusive financial development is thereby reinforced as it expands its access to marginalised groups including women, youth, and informal workers.
- **Conceptual Relationships Among Values, Innovation, and Inclusion**

According to the framework, generational values influence innovation orientation, which in turn affects how inclusive microfinance results are. This relationship between values, innovation, and inclusion shows how generational changes impact microfinance systems and offers a methodical theoretical framework for considering inclusive finance as a development process that is rooted in generations.

1. **Integrating Generational and Sustainability Perspectives in Millennial-Led Financial Innovation:**

Millennial-led innovation in microfinance reflects the convergence of generational values, sustainability principles, and inclusive finance objectives. By integrating these theoretical perspectives, this study explains how millennials promote socially responsible, technology-enabled, and impact-oriented financial solutions that expand access and deepen financial inclusion.

- **Integrating Microfinance and Generational Perspectives**

Financial inclusion is generally explained by microfinance theory through low-income groups' access to loans and basic financial services. However, recent advancements in inclusive finance cannot be adequately explained by this method alone. By emphasising how millennials' common experiences with technology, economic uncertainty, and social responsibility influence their attitude to financial innovation, generational cohort theory deepens the explanation. When these viewpoints are combined, millennial-led microfinance becomes less credit-focused and more value-driven, technology-enabled, and inclusive.

- **Sustainability Theory and Long-Term Inclusion**

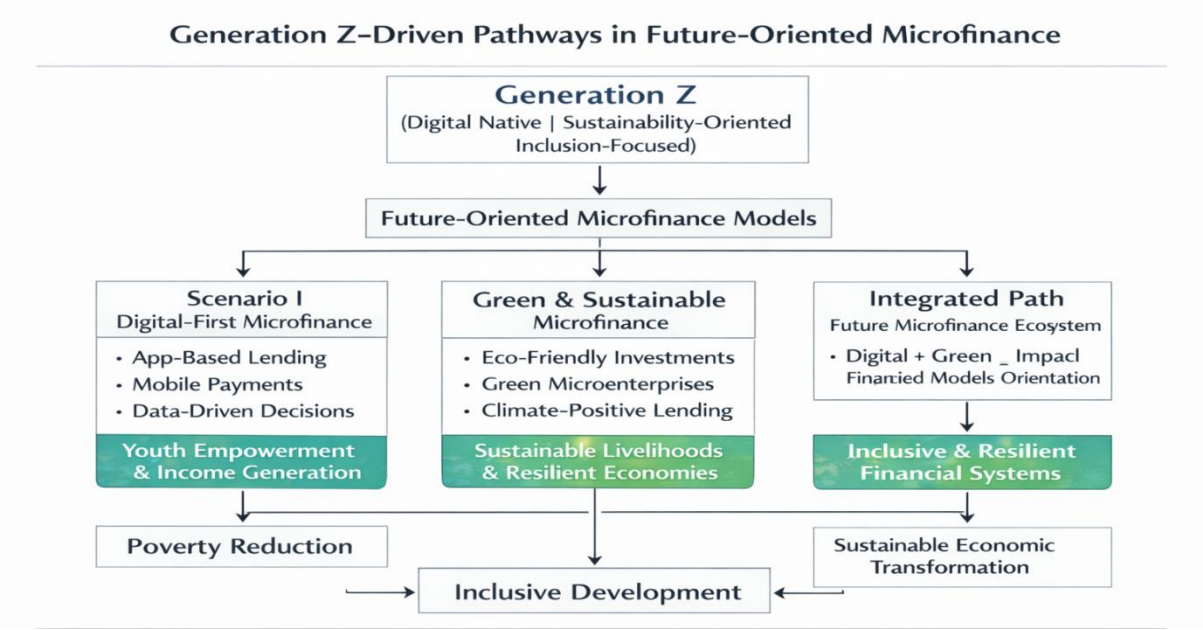
By prioritising long-term social and economic results over immediate financial growth, sustainability theory reinforces this integration even further. By encouraging responsible lending, digital efficiency, and community-level resilience, millennial-led innovations in microfinance are more in line with sustainable development objectives. This theoretical framework explains why millennials prioritise institutional sustainability, financial capabilities, and inclusive design in addition to profitability.

- **Conceptual Synthesis of Theories**

The integrated framework suggests that millennial-driven innovation in microfinance results from the interaction of three theoretical forces. Long-term development perspective is framed by sustainability theory, generational theory describes the innovation attitude, and microfinance theory specifies the inclusion target. When taken as a whole, these theories clarify how microfinance is transformed by millennial leadership into a sustainable and inclusive financial system.

2. Generation Z and Future-Oriented Microfinance for Sustainable Development:

The future involvement of Generation Z in microfinance cannot be explained by linear or static models due to the rapidly evolving technological, economic, and social environment. The investigation of several conceivable scenarios in which Generation Z influences microfinance practices in various but complementary ways is made possible by a scenario-based methodology. Because it reflects uncertainty, innovation potential, and long-term development trajectories, this technique is especially well-suited for conceptual research.



Source: *Compiled by Author*

- **Scenario I: Digital-First Microfinance for Youth Inclusion**

In this scenario, Generation Z drives the expansion of fully digital microfinance models.Gen Z borrowers and entrepreneurs choose mobile-based lending, rapid payments, and platform-driven

financial services since they are digital natives. In response, microfinance organisations implement flexible payback plans, data-driven credit evaluation, and app-based onboarding. By lowering barriers to entry, encouraging youth entrepreneurship, and facilitating the creation of revenue in gig and informal economies, this strategy directly contributes to the elimination of poverty.

- **Scenario II: Green and Sustainable Microfinance Led by Generation Z**

This scenario envisions Generation Z as a catalyst for environmentally sustainable microfinance.Gen Z, which is heavily impacted by social responsibility and climate awareness, supports financial solutions that encourage the use of renewable energy, green livelihoods, and sustainable microbusinesses. Microfinance organisations encourage responsible financing by including environmental factors into lending decisions. This concept links ecological sustainability to poverty reduction, resulting in durable and long-lasting economic development.

- **Scenario III: Ecosystem-Based and Platform-Oriented Microfinance**

In the third scenario, Generation Z transforms microfinance from a stand-alone financial service into an integrated development ecosystem. Microfinance platforms integrate social networks, digital marketplaces, mentorship, and skill development with credit. Peer learning and cooperative entrepreneurship are made possible by Gen Z's dual roles as platform creators and users. This ecosystem-based approach strengthens paths out of poverty by improving employability, market access, and income stability.

CONCLUSION

This study concludes that microfinance should be understood as a dynamic development mechanism that evolves in response to social change, particularly generational change.Microfinance is becoming more and more influenced by the aspirations, attitudes, and technical inclinations of various generations rather than only serving as a method for delivering credit. Through the use of generational cohort theory, the study demonstrates how innovation decisions in microfinance are influenced by generational ideals, which ultimately affect how inclusive and development-oriented financial services become. The study emphasises how important millennials are to the transformation of microfinance practices. Through the integration of digital technology, the emphasis on transparency, and the alignment of financial services with social and developmental objectives, millennial-led approaches have advanced microfinance beyond traditional lending. These modifications, when paired with sustainability theory, help to explain why new developments in microfinance concentrate on long-term social effect, responsible lending, and institutional resilience in addition to financial access. The awareness of inclusive finance as a tool for sustained development rather than a temporary solution to poverty is strengthened by this integrated viewpoint.

The study theoretically views Generation Z as a major force behind the upcoming stage of the development of microfinance. The study uses a scenario-based approach to show how Generation Z might support eco-friendly financial products, digital-first microfinance models, and ecosystem-based platforms that connect finance to markets, networks, and skills. According to these forward-thinking concepts, youth involvement, sustainability, and technology may all be used to simultaneously reduce poverty and restructure the economy. Overall, by presenting inclusive finance as a generationally embedded development process, the work advances theory. By highlighting the necessity of creating adaptable, technologically enabled, and sustainability-

focused microfinance models that are in line with shifting generational ambitions and long-term development goals, it also provides insightful information for policymakers and microfinance organisations.

According to the survey, Generation Z will play a significant role in the next phase of microfinance development. In order to demonstrate how Generation Z might support digital-first microfinance models, eco-friendly financial products, and ecosystem-based platforms that link finance to markets, networks, and skills, the study used a scenario-based methodology. These innovative ideas suggest that technology, sustainability, and youth involvement may all be used to simultaneously decrease poverty and restructure the economy. Overall, the book improves theory by portraying inclusive finance as a generationally embedded development process. It also offers useful information for policymakers and microfinance groups by emphasising the need to establish flexible, technologically enabled, and sustainability-focused microfinance models that are consistent with changing generational aspirations and long-term development goals.

REFERENCES

1. Chibba, M. (2009).Financial inclusion, poverty reduction and the Millennium Development Goals. *European Journal of Development Research, 21*(2), 213–230. https://doi.org/10.1057/ejdr.2008.17
2. Chen, J., Chang, A. Y., &Bruton, G. D. (2017). Microfinance: Where are we today and where should the research go in the future? *International Small Business Journal: Researching Entrepreneurship, 35*(7), 793–802. https://doi.org/10.1177/0266242617717380
3. Hani, U., Wickramasinghe, A., Kattiyapornpong, U., &Sajib, S. (2024). The future of data-driven relationship innovation in the microfinance industry.*Annals of Operations Research, 333*, 971–997. https://doi.org/10.1007/s10479-022-04943-6
4. Sconti, A. (2022). Digital vs. in-person financial education: What works best for Generation Z? *Journal of Economic Behavior& Organization, 194*, 300–318. https://doi.org/10.1016/j.jebo.2021.12.001
5. Haeger, D. L., &Lingham, T. (2014). A trend toward work–life fusion: A multi-generational shift in technology use at work. *Technological Forecasting and Social Change, 89*, 316–325. https://doi.org/10.1016/j.techfore.2014.08.009
6. Tulgan, B. (2004). Trends point to a dramatic generational shift in the future workforce. *Employment Relations Today, 30*(4), 23–31. https://doi.org/10.1002/ert.10105
7. O'Connor, A., &Raile, A. N. W. (2015). Millennials' "get a real job": Exploring generational shifts in the colloquialism's characteristics and meanings. *Management Communication Quarterly, 29*(2), 276–290. https://doi.org/10.1177/0893318915580153
8. Nizam, R., Karim, Z. A., Rahman, A. A., &Sarmidi, T. (2020). Financial inclusiveness and economic growth: New evidence using a threshold regression analysis. *Economic Research–EkonomskaIstraživanja, 33*(1), 1465–1484. https://doi.org/10.1080/1331677X.2020.1748508
9. Chatterjee, A. (2020). Financial inclusion, information and communication technology diffusion, and economic growth: A panel data analysis. *Information Technology for Development*.https://doi.org/10.1080/02681102.2020.1734770

10. Singh, J., &Yadav, P. (2012).*Micro finance as a tool for financial inclusion and reduction of poverty*. ***Journal of Business Management & Social Sciences Research*, 1**(1), 1–12.

11. Abu Daqar, M. A. M., Arqawi, S., & Abu Karsh, S. (2020). *Fintech in the eyes of Millennials and Generation Z: The financial behavior and fintech perception*. **Banks and Bank Systems, 15**(3), 20–28. https://doi.org/10.21511/bbs.15(3).2020.03

12. De Chlarence, J. M., Shanmugam, R., &Rajeswari, P. S. (2022).*Generation Z at workplace*. **Neuro Quantology, 20**(5), 3717–3729. https://doi.org/10.14704/nq.2022.20.5.NQ22669

13. Yap, S., Lee, H. S., &Liew, P. X. (2023).*The role of financial inclusion in achieving finance-related sustainable development goals (SDGs): A cross-country analysis*. **Economic Research–EkonomskaIstraživanja, 36**(3), 2212028.https://doi.org/10.1080/1331677X.2023.2212028

14. Kulmie, D. A., Hussein, M. S., Abdi, B. M., Abdulle, M. A., & Adam, M. A. (2023). *Entrepreneurship training, job creation and youth empowerment*. **Asian Social Science, 19**(6), 111–123. https://doi.org/10.5539/ass.v19n6p111

15. Khan, N., Zafar, M., Okunlola, A. F., Zoltan, Z., & Robert, M. (2022).*Effects of financial inclusion on economic growth, poverty, sustainability, and financial efficiency: Evidence from the G20 countries*. **Sustainability, 14**(19), 12688.https://doi.org/10.3390/su141912688

16. Yang, Y., & Fu, C. (2019).*Inclusive financial development and multidimensional poverty reduction: An empirical assessment from rural China*. **Sustainability, 11**(7), 1900.https://doi.org/10.3390/su11071900

17. Nga, J. K. H., Yong, L. H. L., & Sellappan, R. D. (2010). *A study of financial awareness among youths*.**Young Consumers, 11**(4), 277–290. https://doi.org/10.1108/17473611011093916

18. Lusardi, A., &Oggero, N. (2017). *Millennials and financial literacy: A global perspective*. Global Financial Literacy Excellence Center (GFLEC), the George Washington University School of Business.

19. Berengu, J. B. (2020). *Sustainable economic transformation and inclusive development*. **Journal of Business and Economic Research (JBER)**, 12(2), 45–62.

20. Moindi, A. (2025). *Reducing poverty through financial growth: The impact of financial inclusion and development in emerging economies*. **Journal of Business and Economic Options, 8**(1), 61–76.

21. Choung, Y., Chatterjee, S., & Pak, T.-Y. (2023). *Digital financial literacy and financial well-being.* Finance Research Letters, 58, Article 104438. https://doi.org/10.1016/j.frl.2023.104438

22. Banerjee, A., Chandrasekhar, A. G., Duflo, E., & Jackson, M. O. (2013).*The diffusion of microfinance.* Science, 341(6144), 1236498.https://doi.org/10.1126/science.1236498

23. Pitt, M. M., & Khandker, S. R. (1998). *The impact of group-based credit programs on poor households in Bangladesh: Does the gender of participants matter?* Journal of Political Economy, 106(5), 958–996. https://doi.org/10.1086/250037

24. Kicova, E., Michulek, J., Ponisciakova, O., & Fabus, J. (2025).*When financial awareness meets reality: Financial literacy and Gen-Z's entrepreneurship interest.* International Journal of Financial Studies, 13(3), 171.https://doi.org/10.3390/ijfs13030171

25. Haryono, N., et al. (2023). *Undermining shoestring budget: Financial capability determinants of the millennial generation.* International Journal of Sustainable Development and Planning, 18(4), 1137–1147. https://doi.org/10.18280/ijsdp.180417

Asian Journal of Multidimensional Research
ISSN: 2278-4853 Vol. 14, Issue 12, December 2025 SJIF 2022 = 8.179
A peer reviewed journal

SOCIAL JUSTICE, CASTE AND IDENTITY: A CONTEMPORARY DISCOURSE

Dr. Neha Rani*
*Assistant Professor (Political Science),
Guru Nanak Khalsa College,
YamunaNagar, Haryana, INDIA
Email Id: nehaneval75@gmail.com
DOI: 10.5958/2278-4853.2025.00038.7

ABSTRACT

Caste-based identity and social justice are significant facets of modern Indian society that influence its political dynamics, social structure, and economic environment. Despite strong efforts toward social reform and modernization, the caste system—rooted deeply in history—continues to exert a significant influence on various aspects of Indian life. This research paper presents a fair evaluation of the severity of caste-based injusticein modern India, the dimensions of identity politics, and the effectiveness as well as limitations of social justice policies.
The paper analyzes social structures, the historical origins of caste, modern policies such as reservation and caste census, and the social, economic, and political dimensions associated with identity politics. The study demonstrates that caste identity not only generates inequality of opportunity but also affects political representation, distribution of resources, social status, and self-respect. In light of these conclusions, the paper makes advice for stakeholders, social activists, and legislators to address caste-based disparities and advance Social upward mobility in India. It places a strong emphasis on bolstering legal protections, funding education and skill development, and successfully adopting inclusiveness.

KEYWORDS: *Social Justice, Caste, Identity, Constitution, Law, Policies.*

INTRODUCTION

The term *social justice* refers to the establishment of a condition in which every individual in society receives justice, equal opportunities, equal rights, and equal respect. The principle of social justice has evolved from legal, historical, and philosophical foundations. India, as a multi-caste, multicultural, and multi-religious country, has a particular need for social justice.

Social justice does not merely imply the fair distribution of resources; it also encompasses equal opportunities, dignity, inclusive identity, and self-respect. *Caste* is a social system that assigns identity by birth and influences many aspects of an individual's life, including education, employment, social status, and political representation. Indian society has been affected by the caste system for centuries.

This is not merely an issue of social hierarchy; it is also the root of cultural, economic, and political inequality. The term *identity* here refers to social, cultural, and political identity that individuals or groups either accept themselves or are assigned by society. Identity politics has played a crucial role in bringing caste back into public and political discourse. Therefore, caste and identity play a significant role in both the theory and practice of social justice.

The objective of this paper is to analyze the relationship between caste identity and social justice, examine how policies, political strategies, and social movements attempt to ensure caste-based justice, and identify the challenges that obstruct these efforts.

Historical Background

The Indian caste system, one of the most complex and ancient forms of social stratification in human history, has shaped Indian civilization's dynamics for millennia. Its allusions to jati can be found in ancient texts such as the Rigvedaandvarna (social classes) offer early signs of a hierarchical social structure.

The *varna* system created broad categories such as Brahmin, Kshatriya, Vaishya, and Shudra, dividing society based on occupation and social roles. Issues related to social justice included untouchability, restrictions on social mobility, and social exclusion. During the colonial period, the British attempted to make caste more rigid through caste-based censuses and administrative classifications.

During the freedom movement, social justice emerged as a key concern. Thinkers and reformers such as Dr. B. R. Ambedkar and Jyotirao Phule worked tirelessly to dismantle the caste system and establish equality and rights. All Indian citizens were promised social, economic, and political fairness under the Indian Constitution upon independence. By making provisions for Scheduled Castes, Scheduled Tribe, Other Backward Classes, and other marginalised communities, structural frameworks for justice were established.

Contemporary Nature of Caste Identity in India

Even now, caste identity is an important and deeply embedded aspect of Indian society, influencing social interactions, economic prospects, and political activity. Caste identities remain persistent indicators of social identity, impacting opportunities in life in a variety of ways, even in the face of swift modernisation and urbanisation.
Based on familial ancestry, caste identification is assigned at birth, influencing social standing, resource accessibility, and career prospects. These identities are actively perpetuated in daily social interactions, influencing one's self-perception and interpersonal connections; they are not just relics of the past.

Caste identity is socially maintained through communal networks, marriage, and kinship. While religious organisations and caste-based groups preserve group solidarity, endogamous marriage customs guarantee the continuation of caste identity throughout generations. Despite legal initiatives to advance equality, caste still affects access to wealth, jobs, credit, and land.Lower-caste individuals often face barriers in labor markets, leading to persistent income and wealth disparities. Culturally, caste identity is strengthened through customs, rituals, and social norms such as food restrictions, spatial segregation and notions of ritualistic purity. Stereotypes and prejudices linked to caste are reinforced through media, popular culture, and educational institutions.

In India, caste is a major political factor. At the local, state, and federal levels, it affects voting patterns, party politics, and election results.Political parties mobilize caste groups for electoral gain, making caste-based mobilization a defining feature of Indian democracy. While caste-based reservations and political representation aim to address historical injustices, caste politics can also deepen social divisions and hinder democratic unity.

In education, caste identity affects access, retention, and outcomes. Despite universal education policies, disparities persist across caste groups, with discrimination and stigma limiting access to higher education. In the labor market, caste intersects with gender, class, and regional factors, creating systemic barriers despite legal protections.

In conclusion, Identity of caste persists to be a significant aspect of Indian society, influencing social, political, and economic aspects of life in intricate ways. It takes persistent attention to institutional, cultural, and structural aspects to address caste-based inequalities.

Social Justice Policies: Successes and Challenges

India's social justice policies for Scheduled Castes and Scheduled Tribes—particularly affirmative action and reservation—have led to increased representation in education and government employment, supported by constitutional safeguards. However, challenges such as poor implementation, insufficient funding, and continued discrimination persist.

Constitutional Provisions

1. Articles 15(1) prohibit discrimination based on race, religion, caste, sex, or place of birth.
2. Article 15(4): Permits special arrangements for SCs, STs, and socially and educationally disadvantaged groups.
3. Equal opportunity in public employment is guaranteed under Article 16(1).
4. Article 16(4): Allows backward classes to be reserved for public employment.
5. Article 46: Gives the state instructions to promote the economic and educational needs of SCs, STs, and weaker sections.
6. Seats in Parliament and State Legislatures are reserved for SCs and STs under Articles 330 and 332.
7. Article 335**:** Reservation in services and posts under the Union and States.
8. Article 341**:** Power to specify Scheduled Castes.
9. Article 342: Power to specify Scheduled Tribes.

Achievements of Social Justice Policies

- Strong constitutional safeguards
- Increased representation in lower-level government jobs
- Improved literacy through welfare schemes like the Mid-Day Meal Program
- Economic empowerment through access to financial instruments such as Kisan Credit Cards.

Challenges

- Gaps in implementation due to corruption and lack of resources
- Persistent discrimination despite legal protections
- Debate over the "creamy layer"
- Underrepresentation in higher administrative positions
- Political exploitation of caste identities

- Fragmentation among marginalized groups
- Limitations of identity-based approaches without economic and social equality

Suggestions and Corrective Measures

- Improve quality and access to government schools in SC/ST-dominated areas
- Increase scholarship coverage at all educational levels
- Ensure effective implementation of reservation in educational institutions
- Launch targeted skill-development programs
- Establish SC/ST-specific entrepreneurship incubation centers
- Strengthen reservation in public-sector employment
- Improve accountability under the SC/ST (Prevention of Atrocities) Act
- Conduct legal awareness campaigns
- Create leadership academies for SC/ST youth
- Expand healthcare infrastructure in marginalized regions
- Provide special maternal and child health schemes
- Develop centralized dashboards to monitor welfare schemes
- Mandate caste-disaggregated data collection in budgets and programs

CONCLUSION

Social justice, caste, and identity are deeply interconnected concepts. Caste identity has created profound inequalities in opportunities, social status, political power, and resource distribution in India. Despite efforts by policymakers, courts, activists, and civil society, achieving justice in practice remains challenging.

Future efforts must go beyond legal and political measures to include cultural and psychological transformation. Identity politics should empower marginalized communities rather than deepen divisions. Justice and equality must become part of public consciousness.

This study confirms that the struggle for caste justice is an ongoing process. Policies and laws alone are insufficient; social awareness, collective coexistence, and sensitivity toward inequality are essential for meaningful change.

REFERENCES

- Chaudhary, B. S. (2018). *The Dynamics of Caste Identity and Social Mobility in Contemporary India: A Sociological Analysis*, International Journal of Social Impact, 3(4), 94–105.
- Kumar, R. (2019). *Social Justice: An Analysis*, International Journal of Political Science and Governance, 1(1), 7–9.
- Pathania, G. J., & Jadhav, S. (2023). *Caste Identity and Structure of Threats*, Global Journal of Social Exclusion, 4(1).

- Papana, S. (2023). *The Role of the Caste System in Contemporary India*, IJRAR, 10(1), 54–60.
- Kapoor, R. (2023). *The Caste System in India*, Research Gate.

Editorial Board

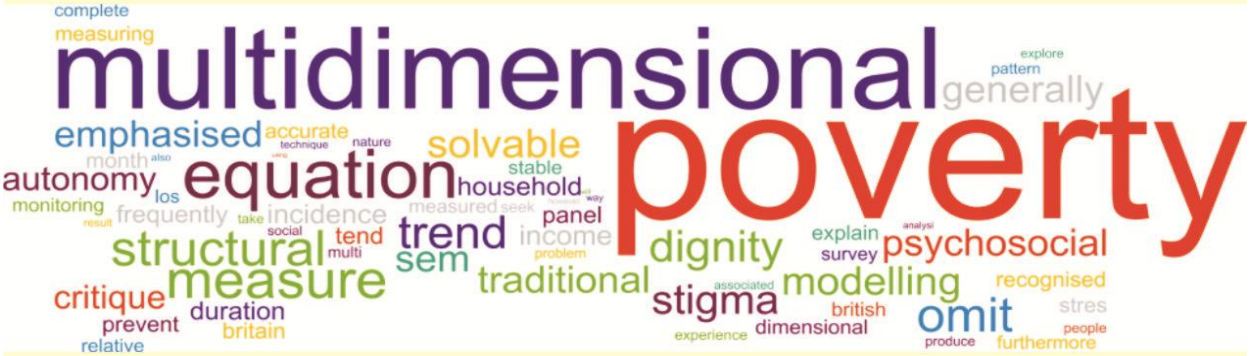
Review Process

Each research paper/article submitted to the journal is subject to the following reviewing process:

1. Each research paper/article will be initially evaluated by the editor to check the quality of the research article for the journal. The editor may make use of ithenticate/Viper software to examine the originality of research articles received.
2. The articles passed through screening at this level will be forwarded to two referees for blind peer review.
3. At this stage, two referees will carefully review the research article, each of whom will make a recommendation to publish the article in its present form/modify/reject.
4. The review process may take one/two months.
5. In case of acceptance of the article, journal reserves the right of making amendments in the final draft of the research paper to suit the journal's standard and requirement.

Categories

- Business Management
- Social Science and Humanities
- Education
- Information Technology
- Scientific Fields



Published by

Trans Asian Research Journals
SCO 34, Ist Floor, HUDA Market,
Near Red Cross, Jagadhri - 135 003 (Haryana) INDIA
Website : www.tarj.in

Our other publications :
Trans Asian Journal of Marketing & Management Research (TAJMMR)
ISSN (online) : 2279-0667