Cogent Business & Management

ISSN: 2331-1975 (Online) Journal homepage: www.tandfonline.com/journals/oabm20

# Stakeholders' understanding of data privacy: implications for digital credit consumer

Saroj Koul, Rakesh Verma & K. V. Ajaygopal

**To cite this article:** Saroj Koul, Rakesh Verma & K. V. Ajaygopal (2025) Stakeholders' understanding of data privacy: implications for digital credit consumer, Cogent Business & Management, 12:1, 2568200, DOI: 10.1080/23311975.2025.2568200

**To link to this article:** https://doi.org/10.1080/23311975.2025.2568200

COGENT BUSINESS & MANAGEMENT
2025, VOL. 12, NO. 1, 2568200
https://doi.org/10.1080/23311975.2025.2568200

MANAGEMENT | RESEARCH ARTICLE

OPEN ACCESS Check for updates

# Stakeholders' understanding of data privacy: implications for digital credit consumer

Saroj Koul[a], Rakesh Verma[b] and K. V. Ajaygopal[b]

[a]Jindal Global Business School, OP Jindal Global University, Sonipat, Haryana, India; [b]Indian Institute of Management Mumbai (IIM Mumbai), Mumbai, Maharashtra, India

**ABSTRACT**

This paper investigates the contextual definition of data privacy among digital credit stakeholders and examines the provisions for data privacy protection in India. This study adopts a primarily qualitative approach, supported by descriptive quantitative data to provide demographic and contextual insights. The data was collected through interviews with key stakeholders (digital credit users (DCUs), digital credit providers (DCPs), and regulatory bodies), supplemented by quantitative analysis of existing data privacy laws and regulations. The study reveals diverse perceptions and understandings of data privacy among stakeholders, influenced by regulatory frameworks, organisational practices, and user behaviours. Existing provisions for data privacy protection in India have varying compliance practices, leading to difficulties in implementation. Adherence to data privacy regulations contributes to the well-being of DCUs, fostering trust, satisfaction, and financial stability. This research underscores the importance of robust data privacy regulations and compliance mechanisms in the digital credit landscape. The findings highlight the need for greater awareness among stakeholders, enhanced regulatory oversight, and tailored interventions to safeguard the privacy rights of DCUs. Qualitative observations and quantitative analysis illuminate the complicated link between regulatory frameworks, organisational practices, and user perceptions. The study offers insights for policymakers, practitioners, and scholars seeking to address the intersection of data privacy and financial inclusion.

**ARTICLE HISTORY**
Received 10 September 2024
Revised 21 September 2025
Accepted 24 September 2025

**KEYWORDS**
digital credit; data privacy; regulatory frameworks; compliance practices; user perceptions; perceived trust; India

**SUBJECTS**
Information Technology; Data Protection; Information Technology Law

## 1. Introduction

The rapidly expanding consumer market, fuelled by the rise of fintech startups, is propelling the growth of digital credit services in India. With a notable increase in the middle class, the Indian consumer market is projected to become the third largest in the world by 2027 (Agarwal, 2023). This development creates a favourable environment for digital credit services to address the rising demand for financial solutions.

The term 'digital credit' describes the use of new technologies and credit scoring algorithms throughout the lending process on digital platforms, from loan application to disbursement **(**Burlando et al., 2024; Ravikumar, 2019). Those who obtain loans via an online platform are called **Digital Credit Users (DCUs),** Digital Credit Borrowers, or Digital Credit Consumers **(**Carlsson et al., 2017; Johnen et al., 2021). Banks license mobile applications known as **Digital Credit Providers (DCPs),** which use online document verification to grant **loans** (Obote, 2023). With programs like 'India Stack' increasing access to financial services and enabling wider availability of credit and financial products, the digital lending landscape in India is expected to grow to a substantial $1.3 trillion by 2030, attributed most notably to the '*Unified Payments Interface* (UPI)' which facilitates mobile fund transfers (IMF (International Monetary Fund), 2021; Economic Times, 2024). India has a thriving fintech scene with over 100 funded digital consumer lending startups offering credit services to various consumer segments, including the informal sector. These include retail cards, gold loans, and the *buy now, pay later* (BNPL) model (Agarwal, 2023).

**CONTACT** Saroj Koul skoul@jgu.edu.in Jindal Global Business School, OP Jindal Global University, Haryana, India.
Supplemental data for this article can be accessed online at https://doi.org/10.1080/23311975.2025.2568200.

Regulatory frameworks governing digital wallets and payment banks are essential to promote innovation, competition, and a safe financial environment in India (IBS Intelligence, 2024). They provide guidelines for customer protection, promote fair practices, and manage risks in the evolving digital financial space.

The financial industry is undergoing a significant transformation, driven by the increasing trend of leveraging data for credit decision-making. The integration of various data and information resources is anticipated to bolster the long-term growth of the credit ecosystem, particularly in allocating resources for credit risk assessment (AMLegals, 2024). As a result, credit risk assessment is progressively incorporating alternative data sources, such as text messages, mobile phone conversations, shopping behaviour, and social media interactions (AMLegals, 2024). Lenders find evaluating credit risk and affordability more challenging without access to accurate real-time data. Therefore, integrating data science and finance has become essential (Forbes, 2023).

For several reasons, data privacy is paramount in the digital credit industry. First, a firm's privacy policy subtly communicates an organisation's dedication to security procedures, which is crucial given the rise in cyber threats (Center for Financial Inclusion, 2022). Second, there can be severe consequences from compromised sensitive data held by financial institutions, which has increased regulatory and public awareness of data privacy. Thirdly, in an increasingly data-driven world, data privacy catalyses trust in digital interactions and protects individuals' fundamental rights **(**Golyan et al., 2024**).** Establishing an atmosphere where users can interact with digital platforms with assurance is essential, knowing their private data is handled with the highest confidentiality. Finally, to build and preserve consumer trust, financial institutions must actively enforce data privacy laws and give them top priority. This commitment entails following privacy laws, implementing strong security measures, and communicating openly about data handling procedures (Forbes, 2023).

Data privacy is crucial in the digital credit industry because it protects customer information, guarantees legal compliance, fosters and preserves customer trust, and reduces the risks of malicious activity and unauthorised access (Forbes, 2023; Golyan et al., 2024). Data privacy, security, and consumer trust are interconnected and have a crucial impact on the digital credit industry. It is mandatory by law and morally right to handle sensitive data responsibly in this context. Consequently, the objective of this research is to examine three significant inquiries:

**RQ 1** What is the contextual definition of data privacy among digital credit stakeholders (**DCU**s, **DCPs**, and **Regulators**) in India?

**RQ 2** What are the provisions for data privacy protection in India?

**RQ 3** How do these provisions impact the **DCUs'** perception of data privacy in India?

This study is critical because it clarifies the crucial data privacy problem in India's rapidly developing digital credit industry. Policymakers, **DCPs**, and consumer advocacy groups can all benefit from the research's understanding of the beliefs and practices of various stakeholders. The knowledge acquired can create more effective data privacy frameworks that safeguard consumers and promote innovation and expansion in the online credit industry. This study contributes to the broader discourse on consumer rights and digital financial services by establishing the foundation for future research and policy formulation.

Structure: The literature review is in Section 2. Section 3 outlines the methodology, and the results are in Section 4. Section 5 discusses the implications of the results. The conclusions with future possibilities are in Section 6, and the reference list is towards the end.

## 2. Literature review

The conceptualisation of data privacy involves ethical considerations, legal frameworks, technological challenges, and implications on user trust and behaviour. The conceptualisation of data privacy involves ethical dilemmas related to gathering and using large volumes of data, including permission, openness, justice, and the impact of data analytics methods on individual privacy rights and societal values (Bruneau et al., 2020). The ethical imperatives observed in previous literature include concerns about privacy,

surveillance, transparency, accountability, trust, equality, discrimination, and justice, which are significant for developing technological, inclusive, and pluralist societies (Drev & Delak, 2022).

Multidimensional Developmental Theory (MDT) (Laufer & Wolfe, 1977) considers privacy as shaped by the interplay of personal, environmental, and interpersonal dimensions, evolving over an individual's life and context. This theoretical lens offers a nuanced understanding of privacy concerns and behaviours by emphasising that privacy is not a static concept but is dynamically constructed across contexts and experiences.

The use of the MDT is justified in the Theoretical Framework due to its nuanced approach to understanding privacy as a dynamic and layered concept, particularly attuned to stakeholders' evolving perceptions in socio-regulatory contexts (Laufer & Wolfe, 1977). MDT differs categorically from alternatives such as the Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT), which focus mainly on technology adoption and lack deep integration of social and regulatory dynamics shaping privacy concerns (Karwatzki et al., 2022). MDT frames privacy as influenced by multiple, intersecting dimensions—self (individual values and identity), environment (social context), and interpersonal relationships—each evolving with stakeholders' experiences, expectations, and regulatory changes (Bartol et al., 2024; Laufer & Wolfe, 1977). This layered structure allows researchers to account for the complexity and continual redefinition of privacy as a social construct, providing insights into how individuals navigate and negotiate privacy boundaries amid shifting technological and regulatory landscapes (Karwatzki et al., 2022).

TAM/UTAUT primarily model technology acceptance by focusing on constructs such as perceived usefulness, ease of use, and behavioural intention, sometimes extended to include privacy or trust; however, they lack the theoretical depth to analyze how privacy perceptions are shaped not just by the technology, but by broader social, developmental, and legal factors that MDT explicitly encompasses (Bartol et al., 2024). MDT explicitly incorporates perceptions of regulation and institutional safeguards as integral to privacy meaning-making, which TAM/UTAUT only address indirectly or via extension (Laufer & Wolfe, 1977; Orszaghova & Blank, 2024). This positions MDT as superior for research questions involving policy, trust, and stakeholder engagement with evolving privacy norms, making it the theoretical choice for studies where the socio-regulatory context is as impactful as the technology itself (Baruh & Cemalcılar, 2014).

Recent studies have revitalised MDT as a conceptual scaffold for analysing privacy in digital contexts. For instance (Bartol et al., 2024), explicitly applies MDT to map how older adults' privacy concerns and perceptions of control are influenced by their lifelong disposition toward privacy, digital environments, and social interactions online. Orszaghova and Blank (Orszaghova & Blank, 2024) employ related frameworks and highlight how privacy motivations and behaviours are neither uniform nor static but are contingent on context, personality, and digital skill, supporting MDT's emphasis on multiple interacting influences. Wang et al. (Wang et al., 2025) further advance this approach by showing how device-specific interactions and evolving digital environments alter privacy boundaries, echoing MDT's core idea that context and technology co-shape privacy perceptions and management.

The legal framework significantly impacts the conceptualisation of data privacy (Figure 1). For instance, the 'European Union's General Data Protection Regulation (GDPR)' seeks to direct the development and use of information communication technology in a way that interferes as little as possible with the privacy of individuals, emphasising 'data protection by design and by default (Gunasekara, 2014; Wang et al., 2025). The United States follows a different approach to data protection than the European Union, and there are ongoing discussions about modernising information privacy law in various countries, including the USA, the European Union, Australia, and New Zealand (Sokolovska & Kocarev, 2018; UNCTAD, n.d.).

Accordingly, 71% of the countries have implemented data privacy legislation, 9% have drafted the legislation, and the rest have no privacy legislation (Zimmer, 2018). The list of all the data protection legislation tabulated by country is provided in Appendix A.

The way data privacy is understood directly influences users' trust and behaviour, which, in turn, affects their willingness to share larger datasets. This requires careful consideration of data ethics and social responsibility, including the importance of transparency, accountability, and trust (Zimmer, 2018).

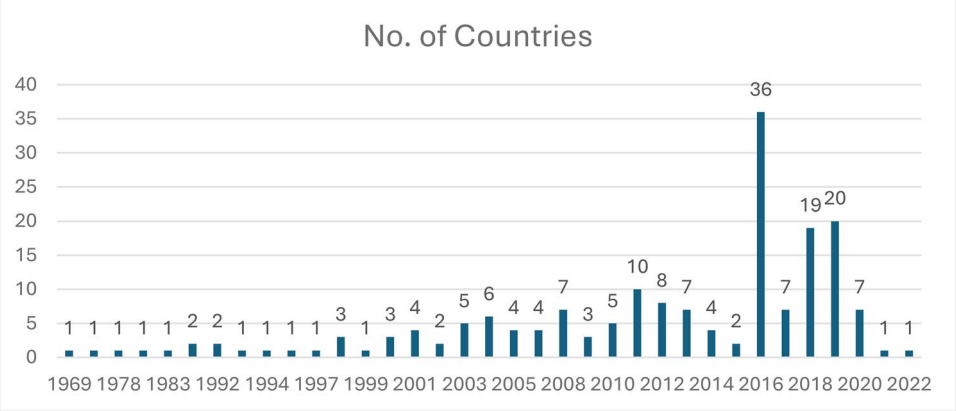



**Figure 1.** Adoption of data privacy policies over the years.

The emergence of big data has created new difficulties in safeguarding information and data privacy. Applying ethical principles to data management and algorithms makes it possible to identify and address ethical dilemmas in data science. This, in turn, directly impacts user trust and behaviour (Parthasarathy et al., 2024).

The existing body of research on data privacy and security investments in organisations, specifically those employing Big Data Analytics (BDA), highlights the need for targeted IT investments in effectively managing total company risk in digitalised environments (Zhang et al., 2021). This sentiment is reflected in conversations around customer views of privacy and the principles of regulatory protection that influence the technology industry, particularly in Artificial Intelligence (AI) development.

Technological research has shown that blockchain, encryption techniques, and safe transaction models protect data security and build customer confidence. Privacy-enhancing technologies play a significant role in achieving these goals (Kandarkar & Ravi, 2024; Rohm & Pernul, 1999). Furthermore, the consequences of adhering to GDPR, experiencing IT security breaches, and using geofence mobile technology in developing economies significantly affect market value, trust-building efforts, and technological integration. These observations shed light on the broader ramifications of data privacy practices (Cheruiyot & Moenyane, 2024; Ford et al., 2023).

Factors affecting consumer perception of data privacy have been studied over time to improve regulatory and policy decisions. Exploring and understanding privacy policies in digital credit usage (Dehling & Sunyaev, 2024; Reidenberg et al., 2016) spotlighted the potential impact of ambiguity in privacy policies. This discussion laid the foundation for identifying the 'Clarity' criterion. However, it's worth considering that a more extensive empirical analysis could bolster the robustness of these findings. Building on this (Brunotte et al., 2023; Majeed, 2023), points out the importance of privacy explanations in cultivating end-user trust, thus contributing to our understanding of the 'Awareness' criterion. However, a broader generalisation beyond social media contexts may be necessary to enhance the relevance of these insights across various digital credit platforms. In their investigation (Bareh, 2022; Bartlett et al., 2023), scrutinised privacy policies to glean insights into algorithmic recommendations, leading us to identify the 'Length' criterion. To further enrich the practical applicability of these findings, a comparative study across diverse **DCP**s might be beneficial.

Authors (Saeed, 2023; Zarifis & Fu, 2023) examined the readability of privacy policies, identifying the 'Readability' criterion. While this study contributes valuable insights, a nuanced analysis of readability in different contexts could provide a more comprehensive understanding. Authors (Zimmer, 2018) further identified the 'Need for Information' criterion by exploring a customer-centric perspective on E-commerce security and privacy. For practical relevance, further exploration of specific information needs could be valuable. Moving forward, authors (Bagwan & Garrido, 2023; Saura et al., 2025) examined privacy concerns within social media communities, shaping our understanding of the 'Communication and Awareness' criterion. A thorough investigation into the effectiveness of awareness measures may be warranted to deepen our insights.

Regarding user concerns (Ho et al., 2023; Majeed & Hwang, 2023), shed light on privacy, distrust, and misinformation, contributing to our identification of the 'Tutorials' criterion. A more extensive exploration

of the effectiveness to better inform practical implications (Sankar et al., 2023; Sharma, 2023) delved into user understanding and perceptions of E-commerce data privacy, guiding our identification of the 'Unauthorised Access' criterion. However, capturing a comprehensive knowledge of unauthorised access concerns may necessitate a more diverse user perspective. Exploring controls (Duggineni, 2023; Pimenta-Rodrigues et al., 2024) offered insights into the impact on data integrity and information systems, informing our 'Disclosure' criterion. While valuable, a nuanced analysis of disclosure practices in various contexts could further enrich these findings. Authors (Bounie et al., 2024; Braulin, 2023) explored the effects of personal information on competition and consumer privacy, contributing to our 'Sale of Personal Information' criterion. Nevertheless, addressing generalisation challenges across different **DCP** and market contexts is an aspect that merits consideration. Furthermore, Abakpa and Dvouletý (2025) noted that the organisational shift towards digital and dispersed work models, such as the widespread adoption of virtual teams (VTs), presents additional layers of complexity for data privacy governance. Their research underscores that VTs, while beneficial for competitiveness and access to global talent, operate with a high degree of technological mediation and face inherent challenges in trust-building and communication (Abakpa & Dvouletý, 2025).

Despite the increasing adoption of digital credit services in India, data privacy concerns remain inadequately addressed in academic literature and regulatory enforcement. While global frameworks like GDPR have established strong precedents for data protection, India's regulatory landscape—guided by the Information Technology Act (2000) and the evolving Personal Data Protection Bill (PDPB)—is still in transition. Existing research on data privacy in digital finance has primarily focused on technical security measures, consumer trust dynamics, and regulatory frameworks; however, there remains a critical gap in understanding how digital credit users (DCUs), digital credit providers (DCPs), and regulators define and interpret data privacy in the Indian context. Prior studies have highlighted the importance of transparent privacy policies, compliance mechanisms, and technological safeguards in fostering consumer confidence. Yet, few have explored how these provisions translate into real-world consumer perceptions and behaviours. This study addresses this gap by examining stakeholder-specific definitions of data privacy, assessing India's existing legal protections, and evaluating their impact on consumer trust, satisfaction, and awareness. By integrating a mixed-method approach, this research not only identifies inconsistencies in policy execution and enforcement but also uncovers the paradox of trust vs. satisfaction, where regulatory compliance does not always equate to consumer confidence. Furthermore, while prior research has primarily focused on cybersecurity risks, this study reveals emerging concerns about unauthorised data sharing and monetisation of personal information, offering new theoretical insights and practical implications for privacy governance in India's digital credit ecosystem.

To summarise, understanding data privacy encompasses exploring ethical concerns, regulatory structures like the GDPR, technological obstacles tackled through *privacy by design*, and the effects on user trust and behaviour. These are all crucial elements that require thoughtful examination. The literature demonstrates a comprehensive approach to comprehending and resolving concerns regarding data privacy through the lens of consumer perception. Hence, this study measures consumer perceptions based on *perceived trust, confidence, satisfaction, experience, and awareness* of DCUs (Table 1). These insights enhance our understanding of the changing landscape of data privacy and its effects on consumers in developing economies.

Hence, it is essential to address important questions about data privacy in India's digital credit context. This includes understanding how different stakeholders define data privacy in this context, analysing the measures to protect data privacy, and assessing how these measures impact **DCUs**. The findings will inform policy recommendations and improve data privacy practices.

## 3. Methodology

To ground this study, we draw on the Multidimensional Developmental Theory (Laufer & Wolfe, 1977), widely recognised as a foundational approach for understanding privacy as a dynamic, contextually embedded construct. Recent work has operationalised MDT's three core dimensions, self-ego, environmental, and interpersonal, in digital privacy, demonstrating that privacy concerns and behaviours reflect lifelong attitudes, the advantages and risks of different technological environments, and ongoing social

**Table 1.** Factors of consumer perceptions.

| Factor | Literature references | Key themes |
|---|---|---|
| Trust | Importance of trust in data privacy; Impact of big data on user trust (Wang et al., 2025; Gunasekara, 2014; Parthasarathy et al., 2024; Ford et al., 2022; Cheruiyot & Moenyane, 2024; Saeed, 2023; Bagwan & Garrido, 2023) | Data ethics, transparency, accountability, and willingness to share data. |
| Confidence | Blockchain and encryption techniques for building user confidence in data privacy. (UNCTAD, n.d.; Zimmer, 2018; Kandarkar & Ravi, 2024; Rohm & Pernul, 1999; Ho et al., 2023; Majeed & Hwang, 2023) | Readability, secure data handling, technological safeguards, and disclosure controls enhance confidentiality. |
| Satisfaction | IT investments in data privacy and their impact on consumer satisfaction; Market value implications of GDPR compliance (Sokolovska & Kocarev, 2018; Parthasarathy et al., 2024; Bartlett et al., 2023; Sankar et al. 2023; Sharma, 2023) | Communication, fair practices, regulatory protection, risk management, and competitive privacy safeguards influence satisfaction. |
| Experience | User experience is shaped by privacy policies, algorithmic recommendations, and clarity of digital credit data handling (Kandarkar & Ravi, 2024; Rohm & Pernul, 1999; Reidenberg et al., 2016; Dehling & Sunyaev, 2023, Saura et al. 2023; Bagwan & Garrido, 2023). | Clarity and readability of privacy policies, algorithmic transparency against breach, policy length, and authorised access. |
| Awareness | Privacy explanations, communication measures, and user-centric privacy perspectives drive awareness (Kandarkar & Ravi, 2024; Rohm & Pernul, 1999; Ford et al. 2022; Cheruiyot & Moenyane, 2024; Brunotte et al. 2023; Majeed, 2023; Bareh, 2022; Bartlett et al. 2023) | Transparent information, explanations of privacy policies, education, and user-centric communication foster awareness. |

negotiations. This perspective allows us to trace the effects of individual privacy dispositions, digital skills, regulatory perceptions, and social support on privacy control and protection strategies. Accordingly, MDT explicitly informs our conceptual framework and hypotheses, and we use its logic to interpret how actors form, adapt, and enact privacy boundaries across various digital settings. The study adopted a mixed-method approach combining a literature review with qualitative and quantitative surveys to provide an understanding of data privacy practices for digital credits in India. Although quantitative data were collected through surveys, these were not analysed using inferential statistical techniques. Instead, they serve to contextualise the qualitative findings by outlining participant characteristics and patterns.

The literature review (Section 2) established the theoretical foundation and identified key themes, including trust, confidence, satisfaction, and India's privacy laws, ensuring the research was grounded in existing scholarship. A quantitative survey was conducted to capture consumer perceptions and behaviours, providing statistical insights into consumer awareness, concerns, and trust in data privacy frameworks. However, quantitative data alone may not fully explain behavioural patterns and policy implications, necessitating a qualitative approach to explore deeper consumer attitudes and regulatory challenges (Dewasiri et al., 2018). The qualitative interviews helped contextualise the survey findings and provided nuanced insights into the impact of India's data privacy laws on consumer confidence in digital credit platforms. By integrating these methods, the study ensures empirical rigour and policy relevance, aligning with best practices in impact evaluations and financial privacy research (Barnow et al., 2024; Dewasiri et al., 2018).

The methodology consists of (Figure 2):

Step 1: Assessment of secondary data to identify the key factors influencing the data privacy protection system.

Step 2: Setting the geographic scope and sample size.

Step 3: Conduct structured in-person surveys and data pre-processing.

Step 4: Analyse responses using NVivo software to aggregate Trust, Confidence, Satisfaction, Experience, and Awareness of **DCU**s towards data privacy.

### *3.1. Identification of key factors and questionnaire preparation*

This section uses collated literature and expert input to identify the key factors affecting digital data policy preferences. This section draws directly on the framework developed by Koul et al. (Koul et al.,

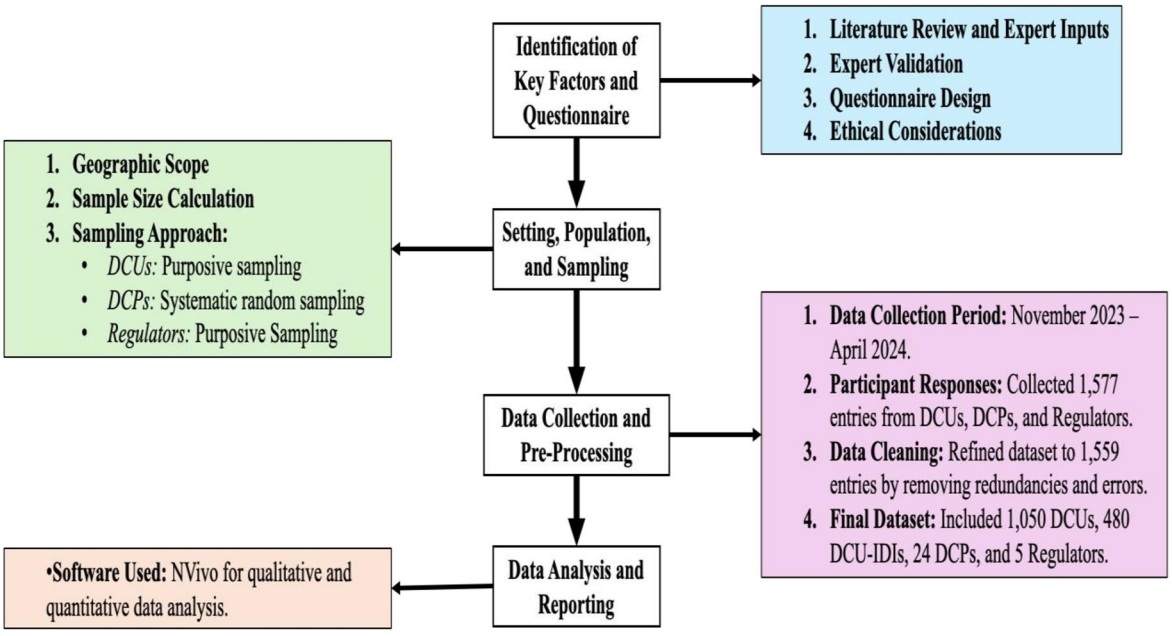



**Figure 2.** Methodological framework of the study.

2024), which identified key factors influencing digital data policy preferences in India's digital credit context. Then, an expert team, at Appendix B, validated the ten criteria from the literature review and proposed three additional criteria. First, they expressed concerns about the perceived lack of control over personal information. Hence, the 'User Control' criterion is included to capture a holistic understanding of the user experiences. Then, concerns about the ability of **DCP**s to delete information upon user request gave rise to 'Capability' criteria. Also, concerns about the availability of options for users to delete personal details contributed to the 'Deletion of User Information' criterion. The exploration of user preferences and the practical implementation of deletion features could enhance these insights.

Hence, the critical factors identified from secondary sources include *Clarity, Awareness, Length, Readability, Need for Information, Measures, Tutorials, Unauthorised Access, Disclosure and Sale of Personal Information*, while the expert team identified and proposed *User control, Capability, and Deletion of user Information* as additional essential criteria.

Step 1: This study employed structured questionnaires comprising open-ended and direct questions to the three key stakeholders of the digital credit ecosystem. They include the **DCU**s, **DCP**s, and the Regulator (Appendix B). While the survey questionnaires have to be rigorous by design and tested to ensure reliable results, they aim to gather detailed insights into people's knowledge, beliefs, attitudes, and behaviours (Koul et al., 2024).

Step 2: Ethical considerations ensured participants' safety and psychological well-being, strengthening the study's quality and credibility (Douha et al., 2023; Koul et al., 2024). The study was approved by the ethics committee of OP Jindal Global University, and their registration number was RERB/2023/089. Authors received 'verbal consent' from 1059 respondents (DCUs), and 'consent in writing' from all 24 DCPs and 5 Regulators who participated in this research. This is further explained under Section 3.3 below.

### *3.2. Setting, population, and sampling*

Based on climatic, geographical, and cultural features, India comprises six zones: North, South, East, West, Central, and Northeast **(**Maps of India, 2023). The prevalence of digital financial services in India is reflected by 370 million live loans in 2022-23 **(**National Payments Corporation of India, 2023; Ministry of Electronics and Information Technology (MeitY), 2023); hence, there is a very high number of **DCU**s. Considering the spread of micro and small businesses and the prominence and diversity of the population that utilises digital credit services, three zones(/regions) will be chosen for this study.

The sample size was determined using the Slovin formula in Equation 1 (Arya et al., 2012; Suresh & Chandrashekara, 2012).

$$n = N / [1 + N(e^2)] \quad (1)$$

where $n$ = sample size, $N$ = the population, and $e$ = margin of error.

With 10% attrition added to these values (Arya et al., 2012; Suresh & Chandrashekara, 2012), the sample size is 341. The sample size denotes the least number of participants deemed representative of a study population. However, this study will attempt to capture a more significant number of participants beyond 341 per region to achieve a more representative sample and broader coverage of the local population.

Public spaces will be pursued in the three zones (regions) (Table 2) to identify **DCU**, such as markets and business centres (unorganised), bus and train stations, worship centres, and recreational centres. In addition, in-depth interviews (IDI) using purposive sampling will be conducted among the DCU. Further, IDI shall be conducted with delegated DCPs and regulators. The prominent regulatory organisations in India are the Reserve Bank of India (RBI) and the Ministry of Electronics and Information Technology (MeitY) (National Payments Corporation of India, 2023; Ministry of Electronics and Information Technology (MeitY), 2023). The role of RBI is to regulate and directly supervise the **DCP**s [also called 'Non-Banking and Financial Corporations' (NBFCs)], ensuring their financial health, compliance with regulatory norms, and contribution to the overall stability and efficiency of the economic system. Per RBI, the number of recognised **DCP**s has varied in the past few years, from 72 (2023) to 441 (2024) (Ministry of Electronics and Information Technology \(MeitY\), 2023; Vasan et al., 2025). From this list, **DCP**s (managerial, operations, and field officers) will be selected for an interview using the systematic random sampling technique, taking every third member.

### 3.3. Data collection and pre-processing

The procedures for selecting respondents from the **DCU** and **DCP** involved using purposive sampling and sending targeted invitations to collect responses for a questionnaire. For **DCU**, a purposive sampling approach based on 1059 data points ensures representation across diverse demographics and usage patterns within the **DCU** population. On the other hand, for **DCP**, 72 invitations to participate in the survey were extended to identified senior-level managers at various **DCP**s. Of these invitations, 24 responses were collected from willing participants in the **DCP** domain. While invitations were sent to 15 regulatory offices, only five (5) agreed to have an in-depth interview. The entire exercise was conducted between November 2023 and April 2024.

Before data cleaning, there were 1,577 entries: 1,059 **DCU**s, 489 **DCU-IDs**, 24 **DCP**s, and 5 Regulators. After cleaning, the dataset was refined to 1,559 entries, consisting of 1,050 **DCU**s, 480 **DCU-IDIs**, 24 **DCP**s, and 5 Regulators. This process eliminated 20 redundant or erroneous entries, improving the accuracy and reliability of the data. Appendix D provides a sample of the collected data.

Of the 1050 Digital Credit Users (DCUs) who participated in the survey, a subset of 480 individuals was purposively selected for in-depth interviews (IDIs). These IDIs were conducted to explore perceptions and experiences that could not be captured through survey responses alone. From this pool of 480 IDIs, a further subset of 120 interviews was selected for detailed qualitative analysis. This final selection was guided by principles of thematic saturation, diversity of perspectives, and representativeness across demographic and geographic categories. The purposive sampling enabled focused qualitative interpretation while ensuring sufficient variation to support the study's analytical objectives. Table 2 reflects this refined subset of 120 DCU-IDIs used in the final analysis.

**Table 2.** Sample size: calculation—qualitative and quantitative.

| Zones (region) | Population (age group: 18–64) | DCU sample size | DCU-IDI sample size | Margin of error |
|---|---|---|---|---|
| NCR | 11530494 | 350 | 40 | |
| East West | 74584967 | 350 | 40 | 0.05 |
| Central | 4,45,15,799 | 350 | 40 | |
| Total | | 1050 | 120 | |

### 3.4. Data analysis

This study adopts a primarily qualitative research design, centred on in-depth, semi-structured interviews with key stakeholders in India's digital credit ecosystems. The qualitative data were analysed thematically using NVivo, following a coding process emphasising iterative comparison and researcher consensus. Employing NVivo for thematic analysis facilitates a structured coding process, enabling researchers to distil complex qualitative data into clear, actionable themes that reflect participant perspectives and contextual realities (Mortelmans, 2019). Inter-coder agreement was regularly checked during the analysis phase, and discrepancies were resolved through discussion to enhance the credibility and trustworthiness of the findings (Paulus, 2023).

For the analysis in NVivo **(**https://lumivero.com), the final 1,558 data points input in Microsoft Excel format shall be analysed. NVivo facilitates the management and analysis of diverse textual and audio-visual materials, aiding in coding, graph creation, and matrix development, thereby enhancing the interpretation of research findings (Mortelmans, 2019**;** Pan & Tang, 2020). Compared to other qualitative data analysis tools, NVivo stands out for its flexibility and comprehensive features, supporting researchers throughout the research process, from literature review to study findings (Limna, 2023; Mortelmans, 2019). Its use also facilitates remote collaboration and reduces costs associated with traditional face-to-face research methods (Mortelmans, 2019; Niedbalski & Ślęzak, 2023).

Quantitative data were limited to descriptive statistics such as participant demographics and frequency distributions, which were provided solely to contextualise the qualitative insights (Appendix C).

## 4. Results

This section presents an in-depth analysis of the rankings and comparisons between **DCU** and **DCP**. All interview transcripts were imported into NVivo 14 software for qualitative data analysis. The process began with open coding, conducted independently by two researchers who systematically reviewed the transcripts to identify recurrent ideas, patterns, and expressions emerging directly from the data.

Initial codes were developed inductively but informed by sensitising concepts drawn from the existing literature, including trust, awareness, clarity, confidence, and satisfaction. These codes were operationalised as NVivo nodes, which were continuously refined as subsequent transcripts were analysed and new insights emerged. The coding structure remained dynamic during the early phases, allowing for the addition, merging, or redefinition of codes as needed. Iterative coding using NVivo, combined with collaborative code development and constant comparison, enhances the reliability of thematic categorisation and the interpretive depth of qualitative findings (Limna, 2023; Pan & Tang, 2020).

Regular meetings were held to discuss coding discrepancies and refine definitions. This iterative process fostered strong inter-coder agreement, which was systematically reviewed and reinforced through discussion until complete consensus was reached on all coding decisions. Subsequently, related codes were clustered into higher-order categories, forming the foundation for overarching themes. For instance, codes such as 'well-informed consent' and 'policy transparency' were aggregated under the broader Awareness theme. In contrast, codes like 'difficulty understanding terms' and 'policy complexity' informed the Clarity theme. Thematic analysis offers a flexible yet rigorous method for identifying, analysing, and reporting patterns within data, especially when researchers engage in an active, reflexive coding process that moves beyond simple description to interpretation (Braun & Clarke, 2006). This process ensured that the themes were empirically grounded and analytically coherent, directly reflecting the participants' perspectives while aligning with the study's research objectives.

To address **RQ1,** all the stakeholders were asked about their understanding of data privacy and digital data privacy through different questions (as in Appendix C2-C4). The contextual definition of digital data privacy among digital credit stakeholders in India and their comparison are given in Tables 3 and 4.

Next, to address **RQ2**, the provisions for data privacy protection in India were reviewed. 'The Digital Personal Data Protection (DPDP) Act of 2023' is India's comprehensive legislation addressing the safeguarding of personal data across many sectors. In August 2023, after several years of discussions, the Indian Parliament passed a law to govern the handling of digital personal data belonging to Indian

**Table 3.** Contextual definition derived from the survey.

| | |
|---|---|
| DCU | Digital data privacy for **DCUs** generally refers to protecting and adequately handling sensitive information provided online to digital credit platforms. This involves ensuring that personal data such as bank account details, Aadhaar numbers, and other sensitive information are confidential and not misused, leaked, sold, or shared without the user's consent. It encompasses the expectation that the data shared online will be safeguarded against breaches, hacking, and unauthorized access, maintaining the integrity and privacy of the user's personal information. **DCUs** expect digital data privacy measures to protect them from fraud, cybercrime, and privacy invasion, ensuring their personal and financial information remains secure. |
| DCP | Digital data privacy, as understood by **DCPs**, encompasses protecting and ethically managing customers' personal and financial information. **DCPs** request personal information to comply with Regulatory requirements, prevent fraud, and offer customized services. This information includes basic personal details, identification documents, proof of address, and income information, all essential for the Know Your Customer (KYC) process. Sensitive data, such as government-issued ID numbers and financial information, are necessary for identity verification and safeguarding against fraud. **DCPs** recognize the risks associated with collecting personal information, such as data breaches, identity theft, and Regulatory non-compliance, and implement robust measures to protect this data. These measures include data encryption, access control, data minimization, regular security audits, and employee training. Furthermore, **DCPs** ensure that any sharing of customer information with third parties complies with data protection regulations, and they typically only share non-sensitive information necessary for service provision. The overall goal is to maintain transparency and gain customer consent while minimizing the risks associated with data collection and processing. |
| Regulators | Digital data privacy, according to **Regulatory bodies**, refers to the protection and ethical handling of personal and sensitive information in the digital realm. This includes ensuring that data collection is minimal and protected, such as using encryption and access control measures. Regulatory bodies emphasize that personal information should only be requested on a need-to-know basis with multiple checks to prevent misuse or unauthorized access. Sensitive data, which encompasses all information that could make an individual vulnerable if breached, must be treated with utmost care and stored securely. Any violation of digital data privacy occurs when personal information is shared or used in violation of established safeguarding principles and Regulatory guidelines, such as those outlined in the IT Act's SPDI Rule (Section 43) or similar data protection regulations. Regulatory bodies, like the Reserve Bank of India (RBI) or the Ministry of Electronics and Information Technology (MEITY), play crucial roles in enforcing these principles and ensuring compliance with data protection laws to safeguard individuals' rights and interests. |

**Table 4.** Difference between contextual definitions.

| | |
|---|---|
| DCU vs Regulator | Digital data privacy for **DCUs** involves protecting and adequately handling sensitive information provided online to digital credit platforms. This ensures that personal data such as bank account details and Aadhaar numbers remain confidential and are not misused, leaked, sold, or shared without consent. **DCUs** expect robust measures to protect their data from breaches, hacking, and unauthorized access, safeguarding their personal and financial information from fraud, cybercrime, and privacy invasion. Regulatory bodies view digital data privacy as the protection and ethical handling of personal and sensitive information in the digital realm. They emphasize minimal data collection, robust security measures such as encryption and access control, and ensuring personal information is requested only on a need-to-know basis with multiple checks to prevent misuse or unauthorized access. Sensitive data must be treated with utmost care and stored securely. Regulatory bodies like the Reserve Bank of India (RBI) and the Ministry of Electronics and Information Technology (MEITY) enforce compliance with data protection laws to safeguard individuals' rights and interests. |
| DCP vs DCU | Digital data privacy for **DCUs** primarily involves protecting and adequately handling their sensitive information, maintaining confidentiality, and preventing unauthorized access. **DCUs** expect robust measures to safeguard their personal and financial information from misuse, breaches, and cyber threats. They emphasize user consent and control over their data, focusing on personal security and ensuring that their information will not be leaked, sold, or shared without their permission. On the other hand, DCPs view digital data privacy as the ethical and secure management of customers' personal and financial information to comply with Regulatory requirements, prevent fraud, and offer customized services. DCPs implement comprehensive security measures, including data encryption, access control, and regular security audits, to protect against data breaches and identity theft. They ensure that data sharing with third parties complies with data protection regulations, aiming to maintain transparency, gain customer consent, and build trust while minimizing data collection and processing risks. |
| Regulator vs DCP | The **DCP** views digital data privacy as safeguarding customers' personal and financial information essential for Know Your Customer (KYC) processes, emphasizing the necessity of sensitive data like government-issued IDs and financial details for identity verification and fraud prevention. They implement robust measures such as data encryption, access control, and employee training to mitigate risks like data breaches and non-compliance with regulations, ensuring transparency and customer consent in data sharing with third parties. In contrast, Regulatory bodies stress minimal data collection, a *need-to-know* basis for personal and sensitive information, and strict enforcement of data protection laws like the SPDI Rule to prevent misuse or unauthorized access, safeguarding individuals' rights and interests across the digital landscape. |

individuals (Braun & Clarke, 2006; Burman, 2023). The DPDP Act envisions establishing a country-wide framework for 'processing personal data' (Naithani, 2025).

The primary objective of this system is to ensure sufficient safeguarding of personal data while ensuring a fair balance between individuals' right to obtain data and processing data for permitted purposes (Burman, 2023; Mortelmans, 2019). Before the DPDP Act in 2023, data protection in the country was governed by the 'IT Act of 2000' and 'IT Rules of 2011', specifically the provisions on 'Reasonable Security Practices and Procedures for Sensitive Personal Data or Information' (Chance, 2023). However, this legislation provided a limited framework for protecting data and guaranteeing privacy (Burman, 2023; Chance,

2023; Mortelmans, 2019). The legislation overhauls the existing fragmented regulations concerning personal data protection and applies to all activities involving digital personal data within India. Furthermore, it can exercise jurisdiction beyond its territory (Burman, 2023; Chance, 2023; Mortelmans, 2019).

The DPDP Act of 2023, India, contains numerous crucial measures (Burman, 2023; Naithani, 2025). The legislation establishes a structure for overseeing digital personal data, excluding data intentionally made publicly available by the person. The consent requirements for processing are limited to consent and particular legitimate purposes. Data fiduciaries who fail to comply with the rules may face financial penalties of up to INR 2500 million (€2.76 million). The Act suggests the creation of a Data Protection Authority (DPA) that possesses extensive authority and implements preventive measures. Data localisation regulations have been loosened, permitting data transmission between jurisdictions. Having 'data processing agreements' is essential before outsourcing to third parties. These regulations safeguard individuals' privacy and personal data while permitting the legal processing of this data (Ministry of Electronics and Information Technology (MeitY), 2023; Burman, 2023; Naithani, 2025).

The DPDP Act, 2023 of India, and the GDPR of the EU have several similarities and differences. The DPDP Act, 2023 pertains explicitly to digital data, whereas GDPR encompasses digital and offline data (scope). DPDP predominantly depends on consent for data processing, but GDPR, apart from consent, includes a broader array of rules. DPDP assigns all compliance duties to Data Fiduciaries, but GDPR imposes direct responsibilities on Data Processors regarding liability (Naithani, 2025; PWC India, 2023). While DPDP imposes penalties for non-compliance 'ranging from INR 500 million (€5.7 million) to INR 2.5 billion (€28 million), GDPR can impose fines of up to €20 million or 4% of the company's global annual turnover from the preceding financial year, whichever amount is higher'. Also, the DPDP Act and GDPR suggest creating an autonomous organisation tasked with executing regulations such as DPA (Naithani, 2025; PWC India, 2023).

The DPDP Act 2023 has significant implications for cross-border data transfers. It allows the transfer of personal data to any unrestricted country (by a Data fiduciary) within the existing laws in India. The DPDP Act provides exemptions for cross-border data transfers if the processing is initiated to enforce the legal rights or claims (individuals), preventing, detecting, investigating, or prosecuting offences or violations of Indian laws. Exemptions apply if Indian courts, tribunals, or other judicial bodies process personal data of individuals outside India, implement schemes of compromise, arrangement, merger, amalgamation, or reconstruction approved by competent authorities, or determine financial information, assets, and liabilities of individuals who have defaulted on financial institution loans. Non-compliance with the DPDP Act's provisions on cross-border data transfers can result in monetary penalties (Burman, 2023; PWC India, 2023). They also offer significant advantages to global businesses, including reduced burdens of adequacy requirements and complex documentation mandated by GDPR (KPMG India, 2023; Latham & Watkins, 2023; PWC India, 2023). Thus, addressing RQ2, the provisions for data privacy protection in India can be concluded as progressive and robust, but they are still in the early stages of implementation.

Lastly, RQ3 examines the impact of provisions on the **DCU**'s well-being. We used NVIVO to code the questionnaire responses, focusing on Trust, Confidence, Satisfaction, Experience, and Awareness of the **DCU** regarding digital data protection and regulatory bodies. The analysis provided in-depth insights into consumer perceptions, as in Figure 3(a–d). The results are organised in Appendix E (E1-E5) and are presented overleaf.

### *4.1. Trust*

- From Appendix E1, survey data reveal that 94% of **DCUs** believe that **DCPs** are transparent about their privacy policies, indicating a generally positive perception of transparency. However, this positive perception is contrasted by significant concerns about security.
- 62% are worried that **DCPs** do not devote enough effort to preventing unauthorised access to personal information. This high level of concern underscores a critical area for improvement in security measures.
- Users also expressed considerable unease regarding the transparency and detail of privacy disclosures. 68% of users find the current disclosures unclear or lengthy. This suggests a need for **DCPs** to

enhance the clarity and conspicuousness of their privacy policies. Additionally, many **DCUs** (63%) are bothered by the extent and nature of data DCPs request. This indicates a significant discomfort with the amount and type of personal information being collected.
- The data shows considerable hesitation among **DCUs** (61%) in providing personal information. This hesitation reflects underlying trust issues and suggests that users are not fully confident in the security and privacy practices of **DCPs**.
- Around 50%–60% of users agree that issues related to collecting, processing, using, and sharing personal information bother them significantly. Specifically, concerns about selling personal information to other companies are high, as per 52% of the users.

The word cloud in Figure 3b visually represents the significant threats and breaches that Indian **DCU**s fear when sharing their data with **DCP**s.

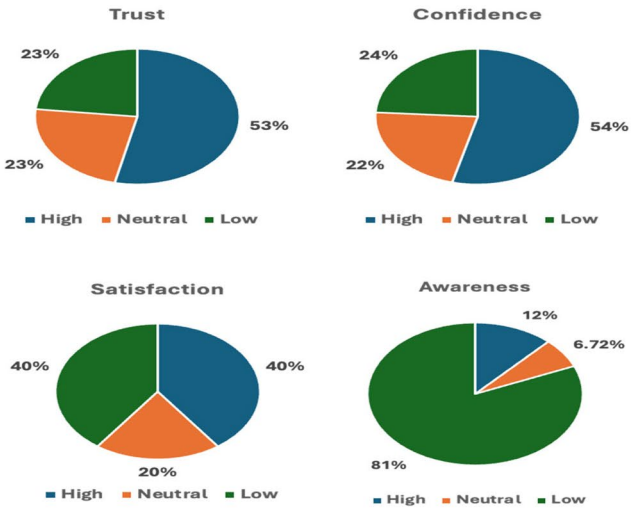
- Prominent terms like 'data breach,' 'fraud,' 'hack,' 'bank,' and 'privacy' underscore significant concerns about security vulnerabilities and fraudulent activities.
- The emphasis on words such as 'account,' 'leak,' 'invasion,' 'theft,' and 'scam' indicates that **DCU**s are particularly worried about unauthorised access and misuse of their sensitive information.
- Specific terms like 'money,' 'details,' 'calls,' and 'Aadhar' (a Unique Identification Number issued by the Government of India) highlight the types of data and communication channels perceived to be at risk.

It is apparent from the results that there is an enormous scope for improving **DCUs'** trust towards **DCPs'** privacy policies. To build trust, **DCPs** need to enhance security measures and improve transparency in their privacy policies. This involves investing in robust security protocols and providing detailed data collection and usage disclosures. Giving users greater control over personal information, including consent and access, is also necessary. Effective communication strategies and compliance with local and international data privacy regulations are crucial for building user trust and satisfaction.

### *4.2. Confidence*

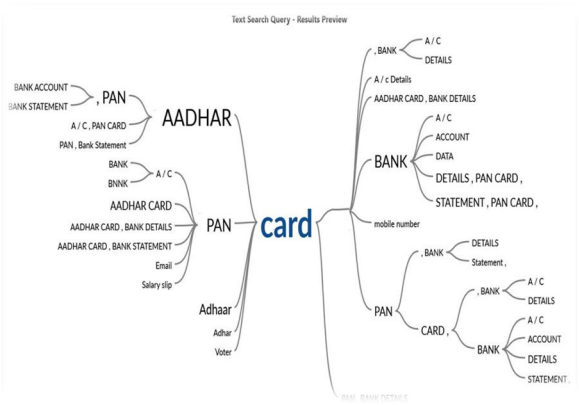
- Appendix E2 shows that 94% of **DCUs** believe that **DCPs** are transparent about their privacy policies. However, despite this perceived clarity, there is notable dissatisfaction with the length and readability of these policies.
- Approximately 73% of users indicate that privacy policies are generally too long, while 69% indicate that these policies are challenging to read.
- A substantial number of respondents (78%) believe that '*more should be done*'. This indicates a significant demand for improved communication and education efforts by **DCPs** to ensure users are adequately informed about their privacy rights and protections.
- Concerns about data deletion are also prominent, with 56% indicating that it bothers them when **DCPs** do not provide the option to delete personal information.
- Similar sentiments are expressed about the lack of a process to request data deletion (54%). Moreover, 53% of users are concerned about whether **DCPs** will 'honour deletion requests', while 50% whether **DCPs** are capable of deleting their information.

In conclusion, while **DCP**s generally have clear privacy policies, their length and complexity negatively impact user confidence. Simplifying these documents to enhance readability and accessibility is crucial. **DCP**s should also adopt more engaging and user-friendly communication methods to raise awareness of privacy policies. Addressing concerns about data deletion with robust processes and ensuring the effective execution of user requests are essential for building trust. By tackling these issues, **DCP**s can significantly improve the confidence of **DCU**s, fostering a more secure and trustworthy relationship and ultimately benefiting the entire digital credit ecosystem.




**a**: Levels of **DCU** perceptions


**b**: Presumed threats to personal data from the perspective of **DCU**




**c**: Sensitive Data in the **DCU** perspective


**d**: Expectation of control of personal data from the perspective of **DCU**

**Figure 3.** (a) Levels of **DCU** perceptions. (b) Presumed threats to personal data from the perspective of **DCU.** (c) Sensitive Data in the **DCU** perspective. (d) Expectation of control of personal data in the perspective of **DCU**.

### 4.3. Satisfaction

- Similarly, Appendix E3 suggests that most **DCUs** believe that **DCPs** take their privacy concerns seriously, with 87.5% of respondents affirming this belief.
- However, a notable minority of 80 respondents do not share this confidence. Additionally, a substantial majority (90%) feel that loan approval models are unbiased, suggesting a general trust in the fairness of the **DCPs**' processes.
- Despite this, 12.5% of respondents indicated they would have reconsidered their loan decisions if they knew their privacy could be breached, highlighting a latent concern about data security.
- Furthermore, many **DCUs** expressed control over their information, with only 80% of respondents indicating no such preference. In contrast, others sought specific settings or policies to manage their data use.
- **DCUs'** opinions on **DCPs** using personal information reveal various views. About 3% are positive, 16% are concerned about potential misuse, and 57% disapprove of practices like selling or sharing data without consent and strongly prefer data protection and minimal sharing.
- Additionally, the responses reflect varying levels of discomfort when providing personal information for loan approvals. About 19% rated their discomfort at the highest level, while 26% felt obliged to share their data, remaining neutral.

In conclusion, most **DCU**s trust that **DCP**s take their privacy concerns seriously and view loan approval processes as fair. However, a significant minority remains concerned about data security and the unauthorised use of personal information. Addressing these concerns through enhanced data protection measures and transparent privacy practices can significantly improve **DCU** satisfaction with **DCP**s' privacy practices.

### 4.4. Experience

- From Appendix E4, a substantial majority expressed positive evaluations. Specifically, 53% of respondents categorised their experience as 'Satisfied' using terms like 'Good' and 'Great.' In comparison, 26% of respondents rated their satisfaction even higher, describing the service as 'Very Satisfied' with terms such as 'Excellent' and 'Very Good.' This indicates a generally favourable perception of the service quality provided by **DCPs** among most users.
- However, a notable segment of users did not share this high level of satisfaction. Seventeen per cent of respondents reported feeling 'Dissatisfied' with descriptors like 'Moderate' and 'Satisfactory,' and a small number (3 respondents) were 'Very Dissatisfied,' citing issues such as lengthy processes and unclear evaluations. Additionally, 4% of respondents maintained a 'Neutral' stance, describing the service as 'Fine' or 'Nice.'

While most **DCU**s expressed positive evaluations of the service, a notable segment reported dissatisfaction due to lengthy processes and unclear evaluations. This mixed feedback highlights the need for **DCP**s to address these issues to improve overall user satisfaction.

### 4.5. Awareness

- Again, from Appendix E5, 53% of users reported being satisfied, describing the service as 'good' or 'great.' In comparison, 26% of users were 'delighted,' using terms such as excellent and very good.
- However, 17% of users expressed dissatisfaction, characterising the service as moderate, fair, or average, and less than 1% of users were very dissatisfied, citing issues such as a lengthy process and lack of clarity.
- Despite the extensive collection of personal data, 42% of respondents indicated no discomfort, though 18% of users felt quite uncomfortable, and 19% felt highly uncomfortable with the data requests.

- Using NVivo, in Figure 3(c), the word tree highlights the personal documents that Indian **DCU**s consider sharing with **DCP**s. The term 'card' is central, indicating its importance. Branches show various related documents: 'Aadhar' and 'Permanent Account Number (PAN)' cards are frequently mentioned, reflecting their significance in identity verification. The 'bank' branch includes 'A/C,' 'details,' 'statement,' and 'account,' emphasizing the necessity of banking information. The connections between 'Aadhar,' 'PAN,' and 'bank' underscore the interlinked nature of these documents. This visualisation shows that **DCU**s are primarily concerned with sharing government-issued identity proofs and banking details with **DCP**s, highlighting the need for secure handling of these sensitive documents.
- The awareness of **DCUs** regarding digital data privacy policies is relatively high, with 69% of respondents indicating they are aware of such provisions in India.
- A substantial majority of **DCUs** are familiar with the existing data protection framework. When evaluating the adequacy and effectiveness of these provisions, a significant portion of users (47.5%) rated them as very good.
- However, a minority (8%) viewed the provisions as ineffective. Nonetheless, there are concerns about implementation quality, with 21% of users expressing poor implementation. These mixed reviews highlight areas where implementation could be strengthened.
- The word cloud analysis in Figure 3(d) highlights key terms regarding how **DCU**s might control shared data with **DCP**s. Prominent words like 'OTP,' 'calls,' 'clear,' and 'transparency' suggest that **DCU**s emphasize the need for clearing or deleting the data from records after using transparent methods such as calling and a 'one-time password' (OTP) for managing data. Concepts such as 'mobile,' 'app,' 'settings,' 'information,' 'options,' and 'technique' indicate a desire for varied and specific control options on mobile applications. Overall, the word cloud underscores the importance of clarity, transparency, and diverse control mechanisms for the **DCU**s to take control of their shared personal data to **DCP**s. OTP is equivalent to a 'verification code' in other countries.

In conclusion, a majority of **DCU**s are satisfied with the service provided by **DCP**s, with many describing it as good or excellent. Despite this, some users expressed dissatisfaction due to issues such as a lengthy process and lack of clarity, and a notable percentage reported discomfort with extensive data collection. The findings emphasise the importance of securely handling sensitive documents like Aadhar, PAN, and banking details. To further enhance user satisfaction, **DCP**s should focus on improving transparency and implementation quality and providing varied control options for data management.

## 5. Discussion

The study sheds light on the varied perceptions and practices regarding data privacy among digital credit stakeholders in India. It reveals that while there are established provisions for data privacy, compliance and implementation remain inconsistent. **DCU**s express concerns about unauthorised access, data breaches, and the lack of control over their personal information. These issues highlight a gap between regulatory intentions and practical execution. **DCP**s acknowledge the importance of data privacy but face challenges in uniformly applying robust security measures. Regulatory bodies emphasise the need for minimal data collection and stringent protection mechanisms, yet the enforcement of these measures appears uneven.

The findings underscore the positive impact of adhering to data privacy regulations on **DCU**s' trust, satisfaction, and financial security. Users who perceive **DCP**s as transparent and proactive in data protection are more likely to trust and engage with digital credit services. However, the study also indicates a pressing need for improved transparency and user education regarding privacy policies, as many **DCU**s feel inadequately informed.

The findings of this study reinforce existing literature on the importance of regulatory clarity and enforcement in shaping user trust in digital credit platforms. Prior research suggests that clear, well-enforced data privacy regulations (such as GDPR) improve consumer confidence in digital transactions (Ford et al., 2023; Kandarkar & Ravi, 2024). However, our study highlights a regulatory-execution gap in India, where policies such as the IT Act (2000) and the proposed Personal Data Protection Bill (PDPB) provide privacy provisions but lack consistent enforcement mechanisms. This aligns with studies

indicating that weak regulatory oversight reduces consumer trust in digital financial services (Barnow et al., 2024; Dewasiri et al., 2018; Latham & Watkins, 2023). Additionally, findings reveal that while DCPs acknowledge the importance of data security (as supported by studies on blockchain and encryption techniques for trust-building (Rohm & Pernul, 1999; Ford et al., 2023; Duggineni, 2023; Pimenta-Rodrigues et al., 2024; Abakpa & Dvouletý, 2025), implementation varies significantly. Many users perceive DCP privacy measures as unclear or insufficient, echoing research highlighting the role of privacy policy readability, transparency, and consumer awareness in trust-building (Bareh, 2022; Bartlett et al., 2023; Saeed, 2023; Zarifis & Fu, 2023). Despite regulatory efforts, this study finds that a lack of accessible privacy information hinders user trust, reinforcing past concerns regarding the ambiguity of privacy policies in digital credit ecosystems (Dehling & Sunyaev, 2024; Reidenberg et al., 2016).

Our findings affirm that privacy is not a monolithic construct, but a multidimensional phenomenon dynamically constructed across personal, environmental, and interpersonal axes, as posited in Multidimensional Developmental Theory (Laufer & Wolfe, 1977). Consistent with (Bartol et al., 2024; Orszaghova & Blank, 2024), we find that variations in privacy skills, perceptions of regulation, and contextual motivations drive distinct patterns of privacy-protective behaviour. Moreover, the device- and time-based nuances in privacy boundaries identified by (Wang et al., 2025) suggest that technical affordances and evolving user practices must be continuously integrated into privacy research and policy design.

While much of the literature suggests that greater regulatory control and technological safeguards enhance trust, our findings introduce a trust vs. satisfaction paradox. Prior research assumes that higher trust leads to higher user satisfaction in digital finance (Brunotte et al., 2023; Gunasekara, 2014; Majeed, 2023; Parthasarathy et al., 2024). However, our study finds that even when users trust that DCPs are secure, they may still express dissatisfaction due to a perceived lack of transparency in data handling. This suggests that satisfaction in digital credit services depends not solely on security but also on user autonomy, data control, and perceived fairness. Another key insight from our findings is that consumer concerns are shifting from security breaches to unauthorised data sharing. Previous literature has predominantly focused on data breaches and hacking threats as primary risks in data privacy (Kandarkar & Ravi, 2024; Rohm & Pernul, 1999; Zhang et al., 2021). However, our study finds that users are equally—if not more—concerned about the unauthorised sale or exchange of their data with third parties. This suggests that future research should expand beyond cybersecurity threats and examine ethical data monetisation concerns.

### *5.1. Implications for policy and practice*

The study's implications for policy and practice are multifaceted. Policymakers must prioritize creating and enforcing comprehensive data privacy regulations adaptable to the rapidly evolving digital credit landscape. Enhanced regulatory oversight is crucial to ensure consistent compliance among **DCP**s. Policymakers should also consider implementing stricter penalties for data breaches and non-compliance to incentivise better data protection practices.

For practitioners, especially DCPs, the study highlights the importance of investing in advanced security measures such as encryption, access controls, and regular security audits. DCPs should strive to simplify their privacy policies, making them more accessible and understandable to users. Developing user-friendly mechanisms for managing consent and data usage can also empower DCUs and enhance their trust in digital credit services. The study also suggests the need for targeted educational initiatives to raise awareness about data privacy among all stakeholders. This includes workshops, webinars, and comprehensive guides that can help users understand their rights and the importance of data protection.

The study's findings align with global discussions on data privacy, where regulations such as GDPR and CCPA have set benchmarks for stronger consumer protection. However, India's evolving **Personal Data Protection Bill (PDPB)** presents unique challenges, particularly in balancing financial innovation with user privacy (Conventus Law, 2024; Latham & Watkins, 2023). Lessons from international frameworks suggest that regulatory clarity, strict enforcement, and consumer education are key to building trust in digital finance ecosystems. Additionally, emerging trends such as decentralized finance (DeFi), AI-driven

credit scoring, and cross-border data flows introduce new complexities to data privacy management. Future regulations should anticipate these advancements by integrating privacy-by-design principles and ensuring that user data rights remain protected in the face of rapid technological innovation.

### 5.2. Theoretical contributions and practical insights

Theoretically, this study contributes to the literature on data privacy in the fintech sector by providing a nuanced understanding of the interplay between regulatory frameworks, organisational practices, and user perceptions. It extends existing theories on data privacy by contextualising them within the Indian digital credit ecosystem, highlighting the challenges and opportunities in this rapidly growing market.

Practically, the study offers valuable insights for various stakeholders. For policymakers, the findings highlight the critical areas where regulatory frameworks need strengthening. For **DCP**s, the study provides actionable recommendations on enhancing data protection practices and improving user trust. For scholars, the research opens avenues for further exploration into the dynamics of data privacy in other emerging markets and the impact of technological advancements on data protection.

Moreover, the study underscores the importance of integrating ethical considerations into data privacy practices. Ensuring transparency, accountability, and user empowerment can significantly enhance the overall effectiveness of data protection measures. By addressing the identified challenges and implementing the recommended strategies, stakeholders can work towards creating a more secure, transparent, and trust-based digital financial environment in India.

In summary, this study not only deepens the understanding of data privacy issues in the Indian digital credit sector but also provides a comprehensive framework for improving policy and practice. The insights gained are crucial for fostering a secure and trustworthy digital financial ecosystem that benefits all stakeholders.

## 6. Conclusion

This study thoroughly examines data privacy in the Indian digital credit ecosystem. It focuses on the perceptions and practices of different stakeholders, including digital credit users **(DCUs),** digital credit providers **(DCPs),** and regulatory bodies. The integration of descriptive quantitative data enhanced the interpretation of qualitative insights, particularly in illustrating the distribution of stakeholder experiences and attitudes.

The investigation reveals that while there are existing provisions for data privacy protection in India, the compliance practices vary significantly among stakeholders, leading to challenges in effective implementation. Despite these challenges, adherence to data privacy regulations positively impacts the well-being of **DCU**s, fostering trust, confidence, and satisfaction, thus enhancing user experience and awareness. The study underscores the importance of robust data privacy regulations and the need for improved regulatory oversight to safeguard the privacy rights of digital credit consumers.

One of the key takeaways from this research is the diverse understanding of data privacy among stakeholders, shaped by regulatory frameworks, organizational practices, and user behaviours. The findings also highlight stakeholders' need for greater awareness and education regarding data privacy. Integrating the Multidimensional Developmental Theory (Laufer & Wolfe, 1977) has provided a robust lens for understanding the complex interplay of individual, social, and environmental factors in shaping privacy behaviours. The evidence underscores that one-size-fits-all solutions are inadequate; interventions must be context-sensitive and account for differences in digital skill, regulatory environment, and social support. These insights are relevant for closing digital inequalities and ensuring more inclusive privacy protection as technologies and use contexts continue to evolve.

Despite its contributions, this study has several limitations. While adequate for initial insights, the sample size may not fully represent the diverse population of **DCU**s in India. Additionally, the dynamic nature of digital credit and data privacy regulations means that findings may quickly become outdated.

Hence, future research should address these limitations by expanding the sample size and including a broader range of stakeholders to enhance the generalizability of the findings. This paper has studied

a limited number of countries where privacy rules are available. As other countries' governments implement privacy rules, comparative studies across regions and other countries could offer a more comprehensive understanding of data privacy in diverse digital credit landscapes. Research could also explore the impact of specific regulatory changes on stakeholder behaviours and trust levels, providing actionable insights for policymakers and practitioners. Further investigation is needed into how different user demographics perceive and respond to privacy risks in digital credit. Comparative studies between India and other emerging economies could provide deeper insights into how regulatory environments shape consumer trust and data security practices. Additionally, future research should examine the economic impact of stricter data privacy enforcement on DCPs and financial inclusion. While privacy regulations enhance user confidence, they may also increase compliance costs for financial service providers, potentially affecting accessibility for lower-income consumers. Exploring the trade-offs between privacy protection and financial inclusion will be critical in shaping balanced regulatory strategies.

In conclusion, this research contributes significantly to the growing body of literature on privacy in fintech by providing a nuanced understanding of the intricate interplay between regulatory frameworks, organizational practices, and user perceptions. The insights gained from this study are vital for informing policy recommendations and enhancing data privacy practices in the digital credit landscape.

## Acknowledgment

The authors thank all the respondents who participated in the survey interviews.

## Authors' contributions

CRediT: **Saroj Koul**: Conceptualization, Data curation, Funding acquisition, Methodology, Project administration, Resources, Supervision, Writing – original draft, Writing – review & editing; **Rakesh Verma**: Conceptualization, Funding acquisition, Methodology, Visualization; **K. V. Ajaygopal**: Data curation, Software, Investigation, Formal analysis, Visualization, Writing-original draft..

## Disclosure statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The authors declare no conflicts of interest.

## Software used

1. NVivo Ver. 14 (https://lumivero.com)
2. Microsoft Office Excel for Windows.

## Funding

The authors appreciate the research funding (in whole or part) from the Digital Credit Observatory (DCO), a program of the Center for Effective Global Action (CEGA), with support from the Bill & Melinda Gates Foundation [INV-032608].

## About the authors

***Saroj Koul*** is a Professor of Supply Chain Management at the Jindal Global Business School, India. Her industry, teaching, and research experience span 35 years. She has to her credit over 35 refereed publications. She has received multiple Research Achievement Awards, Teaching Excellence Awards, and research grants. Her research focuses on system dynamics models, supply chain management, LMICs, BRICS, and organisational communication.

***Rakesh Verma*** is a Professor of Operations Management at the Indian Institute of Management (IIM Mumbai), Mumbai, India. He received his Doctorate in Operations Research from the Indian Institute of Technology, Kharagpur, India. He is a DAAD alumnus. He has to his credit more than 35 refereed publications in journals such as The Journal of Fuzzy Mathematics, Asia Pacific Journal of Operational Research, Physics and Chemistry of the Earth, and International Journal of Soft Computing and International Journal of Business Performance and Supply Chain

Modelling. His research interests include facility location, transportation systems, multiple criteria decision-making, fuzzy MCDM, and supply chain management.

***K. V. Ajaygopal*** is a faculty member at Chanakya University, India, and is pursuing his PhD in Operations and Supply Chain Management at the Indian Institute of Management (IIM Mumbai), Mumbai, India. He has been working in multi-criteria decision-making for the past couple of years. He is a member of ORSI, India, and the International Society on Multiple Criteria Decision Making, USA. He has several academic papers in the pipeline at reputed journals and international conferences. He is also pursuing parallel studies in optimisation techniques, especially large-scale optimisation.

## ORCID

Saroj Koul http://orcid.org/0000-0002-3051-5625
Rakesh Verma http://orcid.org/0000-0002-3637-7788
K. V. Ajaygopal http://orcid.org/0000-0002-4119-7458

## Data availability statement

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

## References

Abakpa, A., & Dvouletý, O. (2025). Navigating the digital era: The role of virtual teams in organisational transformation. *Asia Pacific Journal of Innovation and Entrepreneurship*, *19*(3), 208–233. https://doi.org/10.1108/APJIE-08-2024-0166

Agarwal, M. (2023). India's digital credit wars: Who's thriving & who's striving? [online]. Retrieved September 21, 2025https://inc42.com/features/indias-digital-credit-wars-whos-thriving-whos-strifing/

AMLegals. (2024). Ensuring data privacy in online banking and digital financial services. [online] Retrieved September 12, 2025. https://amlegals.com/ensuring-data-privacy-in-online-banking-and-digital-financial-services/

Arya, R., Antonisamy, B., & Kumar, S. (2012). Sample size estimation in prevalence studies. *Indian Journal of Pediatrics*, *79*(11), 1482–1488. https://doi.org/10.1007/s12098-012-0763-3

Bagwan, F. S., & Garrido, E. D. (2023). Bibliometric analysis of personal data, user privacy, and personal data market (s). In *Big data marketing strategies for superior customer experience* (pp. 100–130). IGI Global.

Bareh, C. K. (2022). Privacy policy analysis for compliance and readability of library vendors in India. *The Serials Librarian*, *83*(2), 148–165. https://doi.org/10.1080/0361526X.2022.2143467

Barnow, B. S., Pandey, S. K., & Luo, Q. E. (2024). How mixed-methods research can improve the policy relevance of impact evaluations. *Evaluation Review*, *48*(3), 495–514. https://doi.org/10.1177/0193841X241227480

Bartlett, M., Morreale, F., & Prabhakar, G. (2023). Analyzing privacy policies and terms of use to understand algorithmic recommendations: The case studies of tinder and spotify. *Journal of the Royal Society of New Zealand*, *53*(1), 119–132. https://doi.org/10.1080/03036758.2022.2064517

Bartol, J., Prevodnik, K., Vehovar, V., & Petrovčič, A. (2024). The roles of perceived privacy control, privacy concerns, and internet skills in the direct and indirect internet uses of older adults: Conceptual integration and empirical testing of a theoretical model. *New Media & Society*, *26*(8), 4490–4510. https://doi.org/10.1177/14614448221122734

Baruh, L., & Cemalcılar, Z. (2014). It is more than personal: Development and validation of a multidimensional privacy orientation scale. *Personality and Individual Differences*, *70*, 165–170. https://doi.org/10.1016/j.paid.2014.06.042

Bounie, D., Dubus, A., & Waelbroeck, P. (2024). Competition and the Two Margins of Privacy. *International Review of Law and Economics*, *83*, 106262. Available at SSRN 4815096.

Braulin, F. C. (2023). The effects of personal information on competition: Consumer privacy and partial price discrimination. *International Journal of Industrial Organization*, *87*, 102923.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bruneau, G. A., Gilthorpe, M., & Müller, V. C. (2020). The ethical imperatives of the COVID-19 pandemic: A review from data ethics. *Veritas Revista de Filosofía y Teología*, *46*, 13–35.

Brunotte, W., Specht, A., Chazette, L., & Schneider, K. (2023). Privacy explanations–a means to end-user trust. *Journal of Systems and Software*, *195*, 111545. https://doi.org/10.1016/j.jss.2022.111545

Burlando, A., Kuhn, M. A., & Prina, S. (2024). The role of credit reports in digital lending: A case study from Mexico. *Oxford Review of Economic Policy*, *40*(1), 104–117. https://doi.org/10.1093/oxrep/grad050

Burman, A. (2023). Understanding India's new data protection law. [online] Retrieved September 9, 2025 https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=enandcenter=global

Carlsson, H., Larsson, S., Svensson, L., & Åström, F. (2017). Consumer credit behaviour in the digital context: A bibliometric analysis and literature review. *Journal of Financial Counseling and Planning*, *28*(1), 76–94. https://doi.org/10.1891/1052-3073.28.1.76

Center for Financial Inclusion. (2022). Why do privacy policies matter for digital credit? [online]. Retrieved September 10, 2025 https://www.centerforfinancialinclusion.org/ why-do-privacy-policies-matter-for-digital-credit

Chance, C. (2023). Digital Personal Data Protection Act: India's new data protection framework" [online]. Retrieved September 9, 2025 https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/08/digital-personal-data-protection-act-indias-new-data-protection-framework.pdf

Cheruiyot, K., & Moenyane, K. (2024). Exploring the potential of adopting geofence mobile technology in the South African retail sector. *Cogent Business & Management*, *11*(1), 2327126. https://doi.org/10.1080/23311975.2024.2327126

Conventus Law. (2024). Data law series 4: Implications of digital personal [online]. Retrieved Sept. 1, 2025, https://conventuslaw.com/report/fig-paper-no-30-data-law-series-4-implications-of-digital-personal-data-protection-act-2023-for-foreign-banks-in-india/

Dehling, T., & Sunyaev, A. (2024). A design theory for transparency of information privacy practices. *Information Systems Research*, *35*(3), 956–977. https://doi.org/10.1287/isre.2019.0239

Dewasiri, N. J., Weerakoon, Y. K., & Azeez, A. A. (2018). Mixed methods in finance research: The rationale and research designs. *International Journal of Qualitative Methods*, *17*(1), 1609406918801730. https://doi.org/10.1177/1609406918801730

Douha, N. G. Y. R., Renaud, K., Taenaka, Y., & Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. *Information & Computer Security*, *31*(5), 545–575. https://doi.org/10.1108/ICS-03-2023-0032

Drev, M., & Delak, B. (2022). Conceptual model of privacy by design. *Journal of Computer Information Systems*, *62*(5), 888–895. https://doi.org/10.1080/08874417.2021.1939197

Duggineni, S. (2023). Impact of controls on data integrity and information systems. *Science and Technology*, *13*(2), 29–35.

Economic Times. (2024). Decoding the growth of the credit market with the evolving digital lending ecosystem in India [online]. Retrieved September 11, 2025 https://bfsi.economictimes.indiatimes.com/blog/decoding-the-growth-of-credit-market-with-the-evolving-digital-lending-ecosystem-in-india/103865286

Forbes. (2023). Digital banking and consumer data privacy concerns [online]. Retrieved Sept. 15, 2025 https://www.forbes.com/advisor/banking/digital-banking-consumer-data -privacy-concerns/

Ford, A., Al-Nemrat, A., Ghorashi, S. A., & Davidson, J. (2023). The impact of GDPR infringement fines on the market value of firms. *Information & Computer Security*, *31*(1), 51–64. https://doi.org/10.1108/ICS-03-2022-0049

Golyan, A., Panchal, S., Vaghasiya, D., & Parekh, H. (2024). Data ethics and privacy. In *Recent trends and future direction for data analytics* (pp. 259–268). IGI Global.

Gunasekara, G. (2014). Paddling in unison or just paddling? International trends in reforming information privacy law. *International Journal of Law and Information Technology*, *22*(2), 141–177. https://doi.org/10.1093/ijlit/eat013

Ho, K. K., Chiu, D. K., & Sayama, K. L. (2023). When privacy, distrust, and misinformation cause worry about using COVID-19 contact-tracing apps. *IEEE Internet Computing*, *27*(2), 7–12. https://doi.org/10.1109/MIC.2022.3225568

IBS Intelligence. (2024). Catering to the digital Indian: 10 Key trends reshaping digital banking in India [online]. Retrieved Sept. 1, 2025 https://ibsintelligence.com/ibsi-news/ catering-to-the-digital-indian-10-key-trends-reshaping-digital-banking-in-india-for-2024/

IMF (International Monetary Fund). (2021). India Stack: Financial access and digital inclusion. [online]. Retrieved September 20, 2025https://www.imf.org/external/pubs/ ft/fandd/2021/07/India-stack-financial-access-and-digital-inclusion.htm

Johnen, C., Parlasca, M., & Mußhoff, O. (2021). Promises and pitfalls of digital credit: Empirical evidence from Kenya. *PloS One*, *16*(7), e0255215. https://doi.org/10.1371/journal.pone.0255215

Kandarkar, P. C., & Ravi, V. (2024). Investigating the impact of smart manufacturing and interconnected emerging technologies in building smarter supply chains. *Journal of Manufacturing Technology Management*, *35*(5), 984–1009. https://doi.org/10.1108/JMTM-11-2023-0498

Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. *Information Systems Journal*, *32*(6), 1126–1157. https://doi.org/10.1111/isj.12386

Koul, S., Verma, R., & Kv, A. (2024). Privacy preferences of consumer and lender: A case of digital credit systems in India. *Journal of Internet Commerce*, *23*(4), 414–444. https://doi.org/10.1080/15332861.2024.2418175

KPMG India. (2023). Digital Personal Data Protection Act, 2023 - KPMG India [online]. Retrieved September 1, 2025. https://kpmg.com/in/en/home/insights/2023/08/digital-personal-data-protection-act-2023-overview.html

Latham & Watkins. (2023). India's Digital Personal Data Protection Act 2023 vs. the GDPR: A comparison [online]. Retrieved September 5, 2025 https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Limna, P. (2023). The impact of NVivo in qualitative research: Perspectives from graduate students. *Journal of Applied Learning and Teaching*, *6*(2), 271–282.

Majeed, A. (2023). Attribute-centric and synthetic data based privacy preserving methods: A systematic review. *Journal of Cybersecurity and Privacy*, *3*(3), 638–661. https://doi.org/10.3390/jcp3030030

Majeed, A., & Hwang, S. O. (2023). The changing landscape of privacy–Countermeasures in the era of the COVID-19 pandemic. *IT Professional*, *25*(4), 52–60. https://doi.org/10.1109/MITP.2023.3287876

Maps of India. (2023). Zonal maps of India [online]. Retrieved September 10, 2024https://www.mapsofindia.com/zonal

Ministry of Electronics and Information Technology (MeitY). (2023). Government of India [online]. Retrieved June 6, 2024 https://www.meity.gov.in/about-meity/functions-of-meity

Mortelmans, D. (2019). Analyzing qualitative data using NVivo. The Palgrave handbook of methods for media policy research. 435–450.

Naithani, P. (2025). Strengthening legitimate use in India's Digital Personal Data Protection Act, 2023. *Global Privacy Law Review*, *6*(Issue 2), 61–65. https://doi.org/10.54648/GPLR2025011

National Payments Corporation of India. (2023). The rise and evolution of India's digital finance [Online]. Retrieved Sept.13, 2024 https://www.npci.org.in/PDF/npci/knowledge-center/partner-whitepapers/The-Rise-and-Evolution-of-India%27s-Digital-Finance.pdf

Niedbalski, J., & Ślęzak, I. (2023). NVivo as a tool for supporting teamwork in the context of qualitative research conducted remotely-opportunities, limitations, and practical tips. In *World conference on qualitative research* (pp. 38–59). Springer International Publishing.

Obote, K. J. (2023). Central Bank of Kenya Prudential Regulations and The Financial Performance of Digital Credit Providers In Nairobi City County.

Orszaghova, E., & Blank, G. (2024). Does the type of privacy-protective behaviour matter? An analysis of online privacy protective action and motivation. *Information, Communication & Society*, *27*(14), 2530–2547. https://doi.org/10.1080/1369118X.2024.2334906

Pan, H., & Tang, L. (2020). Qualitative data analysis in Chinese social science studies -the case of NVivo. *Data Analysis and Knowledge Discovery*, *4*(1), 51–62.

Parthasarathy, S., Panigrahi, P. K., & Subramanian, G. H. (2024). A framework for managing ethics in data science projects. *Engineering Reports*, *6*(3), e12722. https://doi.org/10.1002/eng2.12722

Paulus, T. M. (2023). Using qualitative data analysis software to support digital research workflows. *Human Resource Development Review*, *22*(1), 139–148. https://doi.org/10.1177/15344843221138381

Pimenta-Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., Mendonça, F. L. L. D., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident Visualization and Data Protection Law Review. *Data*, *9*(2), 27. https://doi.org/10.3390/data9020027

PWC India. (2023). The Digital Personal Data Protection Act, 2023 [online]. Retrieved June 10, 2024 https://www.pwc.in/assets/pdfs/consulting/risk-consulting/the-digital-personal-data-protection-act-india-2023.pdf

Ravikumar, T. (2019). Digital lending: Is it an alternative lending revolution? *International Journal of Scientific & Technology Research*, *8*(10), 599–601.

Reidenberg, J. R., Bhatia, J., Breaux, T. D., & Norton, T. B. (2016). Ambiguity in privacy policies and the impact of regulation. *The Journal of Legal Studies*, *45*(S2), S163–S190. https://doi.org/10.1086/688669

Rohm, A. W., & Pernul, G. (1999). COPS: A model and infrastructure for secure and fair electronic markets. In *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32*. IEEE.

Saeed, S. (2023). A customer-centric view of E-commerce security and privacy. *Applied Sciences*, *13*(2), 1020. https://doi.org/10.3390/app13021020

Sankar, J. G., David, A., & Valan, P. (2023). Examining user understanding and perceptions of E-commerce data privacy, security, and protection. In *Confronting security and privacy challenges in digital marketing* (pp. 159–185). IGI Global.

Saura, J. R., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2025). Privacy concerns in social media UGC communities: Understanding user behaviour sentiments in complex networks. *Information Systems and e-Business Management*, *23*(1), 125–145. https://doi.org/10.1007/s10257-023-00631-5

Sharma, S. (2023). *Data privacy concern due to information personalization technologies: A quantitative study, utilizing technology acceptance model (TAM) to explore the consumers' experience in e-commerce* [Doctoral dissertation]. University of the Cumberlands.

Sokolovska, A., & Kocarev, L. (2018). Integrating technical and legal concepts of privacy. *IEEE Access*, *6*, 26543–26557. https://doi.org/10.1109/ACCESS.2018.2836184

Suresh, K. P., & Chandrashekara, S. (2012). Sample size estimation and power analysis for clinical research studies. *Journal of Human Reproductive Sciences*, *5*(1), 7–13. https://doi.org/10.4103/0974-1208.97779

UNCTAD. (n.d.). Data Protection and Privacy Legislation Worldwide. [online]. Retrieved Sept. 2, 2025, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Vasan, S., Rao, A. A., & Gupta, N. (2025). Investigating the opportunities and challenges influencing consumer purchase behaviors and media influence in online food ordering: A thematic analysis. *British Food Journal*, *127*(6), 1984–1998. https://doi.org/10.1108/BFJ-10-2024-1071

Wang, L. H., Rice, R. E., Liu, X., Hagen, I., & Zamanzadeh, N. (2025). Mastering boundaries: Differences in online privacy boundary phenomena across digital devices and years. *Behaviour & Information Technology*, *44*(15), 3750–3770. https://doi.org/10.1080/0144929X.2024.2448706

Zarifis, A., & Fu, S. (2023). Re-evaluating trust and privacy concerns when purchasing a mobile app: Re-calibrating for the increasing role of artificial intelligence. *Digital*, *3*(4), 286–299. https://doi.org/10.3390/digital3040018

Zhang, Y., Zhang, C., & Xu, Y. (2021). Effect of data privacy and security investment on the value of big data firms. *Decision Support Systems*, *146*, 113543. https://doi.org/10.1016/j.dss.2021.113543

Zimmer, M. (2018). Addressing conceptual gaps in big data research ethics: An application of contextual integrity. *Social Media + Society*, *4*(2), 2056305118768300.