CONSUMER DATA SHARING IN URBAN INDIA: THE ROLE OF PRIVACY AND DATA PROTECTION STANDARDS AMONG E-COMMERCE USERS

- Adarsh Philip Roy*

Abstract

In the digital economy, personal data functions as a form of currency for e-commerce platforms. It is in the interest of these businesses to collect as much personal data as possible to further their business interests. But in order to collect personal data legally and ethically, these businesses need to build 'consumer trust'. This empirical study examines the role of data protection standards in shaping the willingness of urban Indian consumers to share personal data with e-commerce platforms. This study draws data through a structured online questionnaire. The research analyses demographic factors, platform usage, and perceptions of regulatory and organisational safeguards. Findings reveal that Indian consumers are platform-fluid. Surprisingly, the study found that data security measures emerged as a more powerful influence on willingness to share personal data. It surpassed factors such as financial incentives and compliance with data privacy laws & regulations. Visible evidence of compliance with international standards, such as ISO/IEC 27701, significantly increased consumer confidence. The study also highlights a persistent gap between consumer awareness and behaviour. Despite recognising the importance of privacy, more than half of the respondents rarely read privacy policies. Concerns about misuse of data and repeated breaches were central. More than half of the respondents stated that they would abandon a platform that has a poor track record of protecting the personal data of their consumers. Notably, multinational corporations did not inherently command greater trust. Consumers prioritised ethical reputations and demonstrable practices over the organisation's geographic scope, size, and capital. The study undoubtedly concludes that trust, through implementation of demonstrable, user-centric privacy-protecting measures when properly communicated and advertised, drives data-sharing

* LL.M. Candidate (Data Science & Data Protection Law) @ WBNUJS, Kolkata (WB). Email: royadarshphilip321@gmail.com

behaviour.

***Keywords**: Data Protection, Consumer Trust, Privacy Standards, Data Science, E-Commerce.*

INTRODUCTION

In the digital age, personal data has emerged as one of the most valuable assets in the global economy, with data being termed the new oil[1]. In the past decade, there has been a rapid expansion of online shopping in India. Urban India has witnessed the most rampant expansion. Technology and e-commerce platforms increasingly collect and process consumer data to deliver personalised services, drive targeted marketing, and enhance user experience. However, with the explosion of online service providers using personal data to achieve their business purposes, there have been increasing concerns among educated Indian consumers about privacy, misuse, and data security.

This study does an empirical investigation into the role of visible data protection practices such as clear privacy policies, compliance disclosures, and technical and organisational safeguards in influencing the willingness of urban Indian consumers to share personal data with tech and e-commerce multinational corporations (MNCs). The research focuses specifically on users from urban India. This target population was selected as residents of urban India have higher access to the internet and digital literacy[2]

The primary aim of this empirical study is to ascertain whether consumers are more willing to share personal data when the platform to which they are sharing personal data complies with recognised data protection standards. Data protection standards may be statutory standards that the organisations have to comply with, as well as standards such as the ISO/IEC 27001 for Information Security Management, ISO/IEC 27701 for Privacy Information Management, and/or the ISO/IEC 27002 for information security controls.

This research also delves into the question of what types of data consumers are willing to share and for what reasons. By analysing both quantitative and qualitative responses collected through an online questionnaire, this study provides valuable insights into the expectations and concerns of Indian consumers regarding data privacy in the digital marketplace.

CONCEPTUALISATION

[1] "The world's most valuable resource is no longer oil, but data", *The Economist*, May 6, 2017, *available at*: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited on: Aug. 29, 2025).
[2] NIIT Foundation, "Bridging the digital divide: Empowering rural India" (2024), *available at*: https://niitfoundation.org/bridging-the-digital-divide-empowering-rural-india/ (last visited on Aug. 16, 2025).

In today's modern day and age, the exponential growth of e-commerce and the internet has fundamentally changed how consumers interact with businesses. Consumers are leaving behind traditional physical routes of shopping by entering new and advanced online methods of shopping. Online shopping means and includes both traditional e-commerce purchases, which may involve delivery times of several days, as well as quick commerce ultra-fast delivery services like Blinkit and Swiggy, which can deliver products within minutes. With this transformation, personal data has emerged as both a currency and a concern.

For a digital platform that relies on a huge number of consumers to gain profits, personal data becomes an integral part of its business model. In such a situation, the notion of 'trust' becomes central to this dynamic as digital platforms have to collect sensitive personal data from their customers to deliver services promptly and achieve their business objectives. Trust, in the context of consumer behaviour, refers to the willingness of consumers to be vulnerable to the actions of a digital platform based on the belief that the platform will act in a responsible manner with their personal data[3].

Acting in a responsible manner means adopting and implementing responsible data governance practices, which can include maintaining confidentiality of the personal data shared, non-exploitation of personal data, compliance with relevant laws and transparency in the data handling practices[4]. The willingness to share personal data, exhibited by customers, is a direct outcome of responsible data governance practices[5]. Personal data can be further classified into personal data and sensitive personal data. Personal data can include basic identifiers such as name and Email ID of the consumer, while sensitive personal data can include data such as location, financial details, or preferences of the consumer. Sensitive personal data should be handled with utmost care as its unauthorised disclosure can lead to substantial damages to the individual.

Indian consumer are more aware of their data privacy rights now than before[6]. Earlier,

[3] eMudhra, "Digital trust and consumer behaviour: Understanding the connection", *available at*: https://emudhra.com/en-my/blog/digital-trust-and-consumer-behaviour-understanding-the-connection (last visited on: Aug. 16, 2025).
[4] SAP, "What is data governance?", *available at*: https://www.sap.com/slovenia/products/data-cloud/master-data-governance/what-is-data-governance.html (last visited on: Aug. 16, 2025).
[5] Conrad Ziller and Benedikt Loepp et al., "Willingness to share personal data online: The role of social influence and sustainability" 83 Technology in Society 102974 (2025).
[6] PwC India, "Only 16% consumers in India understand the Digital Personal Data Protection (DPDP) Act: PwC India survey" (Oct. 21, 2024), *available at*: https://www.pwc.in/press-releases/2024/only-16-consumers-in-

privacy was seen as an afterthought. Today, it stands out as a legal right as well as a competitive differentiator.

Therefore, this study rests on the hypothesis that urban indian e-commerce shoppers are more willing to share personal data when e-commerce platforms provide visible compliance with data protection standards.

SUMMARY OF RELEVANT LITERATURE

Consumer Trust in Digital Environments

Trust has always been the cornerstone of social and commercial exchange. However, in the 21st century, a substantial portion of commercial transactions is done over the internet electronically. This, however, leads to a trust deficit as online transactions, unlike traditional commercial transactions, are mediated facelessly. This artificial distance between the two contracting parties amplifies concerns about opportunism and fraud. Therefore, commercial businesses must create trust with their users. This 'trust' goes beyond ensuring the business transacts with utmost good faith. A trusted organisation also ensures that the personal data of its users is protected and safeguarded. Trust in e-commerce serves as a mechanism for reducing perceived uncertainty and vulnerability, enabling transactions that would otherwise not occur[7].

Structural assurances such as legal protections, certification seals, as well as technological safeguards significantly influence initial trust formation with users[8] However, the mere existence of a privacy policy on the website of a business is insufficient to instil trust. The defining factor is the user's perception of the enforceability of the policy and transparency with which the organisation is operating[9].

Another lesser-known and talked-about dimension of consumer trust is the role of reputation and word-of-mouth in building consumer trust. Various studies have shown that trust for e-

india-understand-the-digital-personal-data-protection-dpdp-act-only-9-indian-organisations-report-a-comprehensive-understanding-of-the-act-pwc-india-survey.html (last visited on Aug. 16, 2025).

[7] Paul A. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model" 7 *International Journal of Electronic Commerce* 69-103 (2003).

[8] Wei Sha, "Types of structural assurance and their relationships with trusting intentions in business-to-consumer e-commerce" 19 *Electronic Markets* 43-54 (2009).

[9] Ardion Beldad and Menno de Jong et al., "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust" 26 *Computers in Human Behavior* 857-869 (2010).

commerce and online platforms is built by peer reviews, ratings and brand reputation as they indicate reliability[10].

Another notable concept on the topic of consumer behaviour in a digital environment is the concept of 'privacy paradox'. This is a phenomenon in which users exhibit concern for their own privacy but end up disclosing personal information for convenience or for small rewards[11].

In the digital domain, consumer trust is built through perceived security measures, transparency in data handling practices, and adherence to privacy standards. The absence of these trust-building elements can lead to scepticism and reluctance among consumers to share their personal data. This reluctance will cost the platform valuable consumer engagement[12].

Data Protection Regulations and Their Impact

The proliferation of the internet and increasing adoption of technology on a large scale by people have prompted governments worldwide to legislate on data privacy regulations.

The primary aim of such legislation is to protect the personal data of the residents of the respective jurisdictions. However, governments cannot place heavy, unattainable standards of data privacy and protection on private entities because it may stifle innovation and hinder economic growth. Personal data is indispensable for an organisation to grow in this modern world characterised by rampant technological adoption. Therefore, governments that restrict businesses from sourcing personal data shall pay hefty prices in the form of a weakened economy. Therefore, the law has to balance innovation and economic growth with the need to safeguard the data privacy rights of its citizenry.

The GDPR of the European Union is typically seen as the gold standard for data privacy by privacy professionals worldwide. Studies have shown that visible compliance with GDPR has

[10] Roger C. Mayer and James H. Davis *et al.*, "An integrative model of organizational trust" 20 Academy of Management Review 709-734 (1995).
[11] Alessandro Acquisti and Laura Brandimarte et al., "Privacy and human behavior in the age of information" 347 Science 509-514 (2015).
[12] M. B. Cetin, "Evaluating the effects of digital privacy regulations on user trust" (2024), *available a*t: https://arxiv.org/pdf/2409.02614 (last visited on: Aug. 16, 2025).

shown tangible effects on consumer trust and willingness to share personal data[13]

In India, the DPDPA, 2023 (Digital Personal Data Protection Act) enforces key data privacy principles such as obtaining valid consent, data minimisation, data limitation, etc. The Act also proposes the creation of a data protection board to oversee compliance. Scholars and legal experts have, however, opined that the effectiveness of the regime will ultimately depend upon the capacity of the regulator to implement the legislation and monitor compliance. A survey conducted by PwC India in 2024 found that 82% of Indian consumers cited data protection standards implemented by organisations as a critical factor in building brand trust[14]. This survey revealed the growing awareness among indian consumers with respect to data privacy. The implementation of DPDPA is expected to influence consumer behaviour further.

Consumer Behaviour and Data Sharing

Consumers' data sharing behaviour is primarily influenced by factors such as privacy trust and control over their personal data. Digital personal data is often shared as an additional form of currency, as it has inherent economic value. Therefore, studying and analysing how and why data is shared is imperative. Consumers share personal data based on the potential benefits of such disclosure, which researchers have termed the *privacy calculus*[15]. The idea is that consumers weigh the benefits they may derive from sharing personal information against the possibility of their data being misused. After making a risk-benefit analysis, they make a rational decision based on the individual's best interest.

Research has also indicated that privacy concerns and users' risk-benefit psychological analysis are contextual. The sensitivity of the requested information and the trustworthiness of the organisation requesting information determine consumer decisions[16]. Sensitive information, such as biometric and financial data, is scrutinised heavily by users when

[13] Grace Fox and Theo Lynn et al., "Enhancing consumer perceptions of privacy and trust: a GDPR label perspective" 35 *Information Technology & People* 181-204 (2022).
[14] PwC India, "82% of Indian consumers consider protection of personal data as most crucial factor in building trust: PwC's Voice of the Consumer Survey 2024" (July 11, 2024), *available at*: https://www.pwc.in/press-releases/2024/82-of-indian-consumers-consider-protection-of-personal-data-as-most-crucial-factor-in-building-trust-pwcs-voice-of-the-consumer-survey-2024.html (last visited on Aug. 16, 2025).
[15] H. Zhu and C. X. J. Ou et al., "Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making" 54 *Information & Management* 427-437 (2017).
[16] *Supra* note 11.

compared to other less sensitive personal data, such as Email addresses.

It has also been found that consumers tend to share more personal data when they receive tangible benefits. Tangible benefits can mean discounts or personalised services, etc[17]. However, this willingness is contingent upon the assurance that their data will be handled responsibly.

Another important dimension of consumer data sharing behaviour is transparency and control. Users tend to share more personal data when they are informed how exactly their data is collected, how it is used and stored and how it will be deleted after the purpose is served[18]. Similarly, offering a granular control mechanism to users will enhance user perception of the service[19]. This can include mechanisms such as opt-in consent mechanisms. However, it is to be noted that this can lead to a well-documented phenomenon called 'consent fatigue'.

Challenges in Building and Maintaining Trust

Trust, if established by an organisation with its customers, can be a powerful tool to increase customer engagement and loyalty. However, trust is fragile and can be easily eroded by missteps. Numerous ongoing challenges prevent organisations from building and maintaining trust. Data breaches, misuse and exploitation of personal data and lack of transparency can erode consumer trust rapidly[20]. A good example of this is the Tata Neu case. Tata Neu was a super app that faced immense criticism from privacy advocates. Tata Neu pre-populated the Tata Neu apps from other apps offered by the Tata Group, such as Big Basket, into the Tata Neu app. This included personal data such as addresses and other details without explicit user consent[21]. Research has consistently shown that misuse of data and data breaches have

[17] D. Bae and R. Mayya *et al.*, "Privacy Regulation and Its Unintended Consequences on Consumption Behaviours: Evidence From CCPA", Platform Strategy 2023 Conference, Boston University Questrom School of Business, June 2023, *available at*: https://questromworld.bu.edu/platformstrategy/wp-content/uploads/sites/49/2023/06/PlatStrat2023_paper_108.pdf (last visited on Aug. 16, 2025).
[18] Heng Xu and Tamara Dinev et al., "Information privacy concerns: Linking individual perceptions with institutional privacy assurances" 12 *Journal of the Association for Information Systems* 798-824 (2011).
[19] Huseyin Cavusoglu and Tuan Q. Phan et al., "Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook" 28 Information Systems Research 457-481 (2017).
[20] Mamta Kumari and Pallav Chandra Sinha et al., "The impact of data breaches on consumer trust in e-commerce" 4 International Journal of Computer Science and Technology 2014.
[21] Wired, "India's New Super App Has a Privacy Problem" (2022), *available at*: https://www.wired.com/story/india-tata-super-app-privacy (last visited on: Aug. 16, 2025).

eroded consumer trust and undermined brand reputation, even if subsequent remedial measures were undertaken to rectify[22].

Another major issue facing organisations in building effective trust with their users is a phenomenon known as 'consent fatigue'. The complexity with which organisations acquire consent through complex privacy policies and consent mechanisms can lead to consumer fatigue. In such a situation, the consumers consent to data sharing without fully understanding the implications of what they're consenting to[23]. Therefore, even if users technically consented to a particular data processing, they might feel betrayed as they might 'feel' that they did not consent to the processing. This thought process within the consumer stands in the way of effective trust building with an organisation.

Another Major concern that consumers have that prevents them from building trust with businesses is the gaps that exist in reality with the regulatory rights and their enforcement. Consumers can remain sceptical about abstract legal assurances[24]. This issue is particularly true in a country like India, where bureaucratic efficiency & corruption are perceived to be rampant.

Finally, the cultural and behavioural nature of consumers in general also affects the trust-building process. In India, we can see a general mistrust of MNCs and new technology. Consumers could feel that MNCs are exploitative, and new technologies are tools for exploitation and independent certifications as manipulation methods.

The Role of Organisational Practices

Organisational practices concerning data protection are policies, routines, and behaviours that an organisation follows that delineate how personal data is collected, processed, stored and eventually deleted or archived. Every organisation has its own unique organisational practices with respect to data protection. Some organisations choose to design their

[22] Ponemon Institute LLC, "The Aftermath of a Data Breach: Consumer Sentiment" (Apr. 2014), *available at*: https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf (last visited on: Aug. 16, 2025).
[23] Center for Information Policy Leadership, "The limitations of consent as a legal basis for data processing in the digital society" (Dec. 2024), *available at*: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf (last visited on: Aug. 16, 2025).
[24] *Supra* note 9.

organisational practices in tune with regulatory requirements. However, we can see various organisations in India implementing more sophisticated data protection practices to get a strategic advantage in the market. These strategic undertakings can take the form of adequate & effective cybersecurity safeguards, conducting regular personal data audits, and being transparent about the data handling practices of the organisation[25].

Transparency in personal data handling practices is one of the leading organisational best practices that builds consumer trust. Openness in explaining how data is handled and proper communication of practices help bridge the trust gap between organisations and consumers. Research has also shown that even if openness shows the limitations suffered by organisations, it is a net positive for the organisations.[26] In conclusion, we can say that organisational practices are the operational backbone of an organisation.

OBJECTIVES

With increasing awareness of data privacy and the implementation of data protection regulations, understanding the determinants of consumer trust and behaviour becomes crucial, especially in the context of tech and e-commerce multinational corporations (MNCs).

The study's specific objectives are:

1. To identify the specific factors influencing urban Indian online shoppers' willingness to share their personal data.
2. To investigate the relationship between data protection measures and consumers' willingness to share personal data, if any.
3. To analyse the effectiveness of data protection measures implemented by tech and e-commerce MNCs in influencing the willingness of consumers to share personal data.
4. To determine the willingness of urban indian online shoppers to share additional personal data in exchange for personalised services and benefits.

[25] IAPP, "Operationalising India's new data protection law" (2023), *available at*: https://iapp.org/news/a/operationalizing-india-s-new-data-protection-law-the-challenges-opportunities-ahead (last visited on: Aug. 16, 2025).
[26] Han Li, Rathindra Sarathy & Heng Xu, "Understanding situational online information disclosure as a privacy calculus" *Journal of Computer Information Systems* (2010) (forthcoming).

5. To assess consumer trust in multinational corporations.
6. To identify the primary concerns of consumers when sharing personal data on e-commerce platforms.
7. To determine the extent of consumer awareness and perception of the effectiveness of specific data protection measures.
8. To assess the long-term impact of repeated data breaches on consumer trust and brand loyalty.

By addressing these objectives, this study aims to provide insights for business organisations and other stakeholders seeking to build a trust-driven, privacy-respecting digital ecosystem in India.

METHODOLOGY

The researcher has followed a systematic methodology that ensures that the data collected is relevant and accurate. The methodology followed is suitable for deriving meaningful conclusions that align with the objectives that the study seeks to address.

- The universe of the study comprises online shoppers residing in urban areas across India. Among the urban online shoppers, the consumers who use e-commerce platforms and tech applications for purchasing goods and services are the primary focus. The population of the study includes individuals of varying ages, professions, and educational backgrounds who have access to the Internet and engage in digital transactions.
- This study employs a quantitative and exploratory research design, supplemented with qualitative elements.
- The sampling method chosen by the researcher is the non-probability convenience sampling.
- The sampling method adopted for the study is the non-probability convenience sampling. This sampling method was chosen owing to time and accessibility limitations.

- Respondents for the study were primarily drawn from social media platforms and personal connections. The methods of sourcing responses for the questionnaire included LinkedIn connections, student networks, and professional groups.
- The data for the study were collected using a structured questionnaire designed through Google Forms. The form consisted of both multiple-choice and open-ended questions. This allowed for both statistical analysis and thematic interpretation.
- All respondents remained anonymous, and their consent was presumed upon submission of the form.
- The interpretation of data focused on linking empirical findings to the theoretical framework developed in the conceptualisation section of this study.
- This study is limited to Business-to-Consumer (B2C) transactions and does not cover Business-to-Business (B2B) interactions.

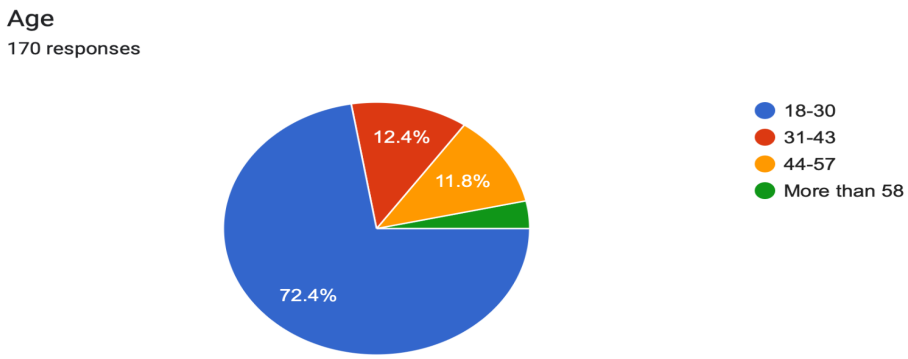
FINDINGS OF THE STUDY

This section presents the study's key findings. The findings are interpreted and assessed with the help of visualisation tools that were readily available through Google Forms. The following subsections provide a detailed breakdown.

Demographics

This subsection consists of information and analysis about the demographic profile of the respondents. It includes their age, occupation, and educational qualifications. Understanding this information is crucial in contextualising the collected data.

Age Distribution

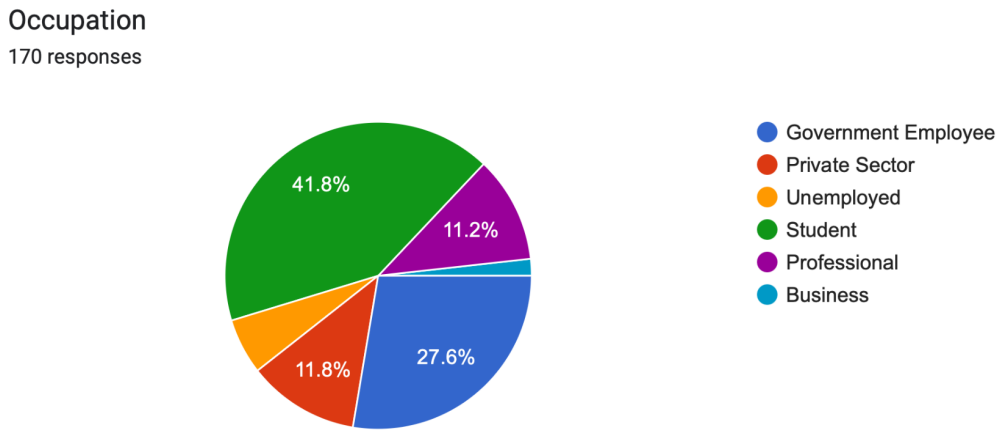


- 72.4 % of respondents were young adults aged 18-30, and they form the dominant demographic of this study.
- However, other age categories were decently represented in this study, with middle-aged Indians in the age category 31-43, forming the second biggest demographic.

Implications:

- As the study focuses on urban online shoppers in India, the age skew towards younger demographics is expected. This is so because they are the most active digital consumers.

Occupation



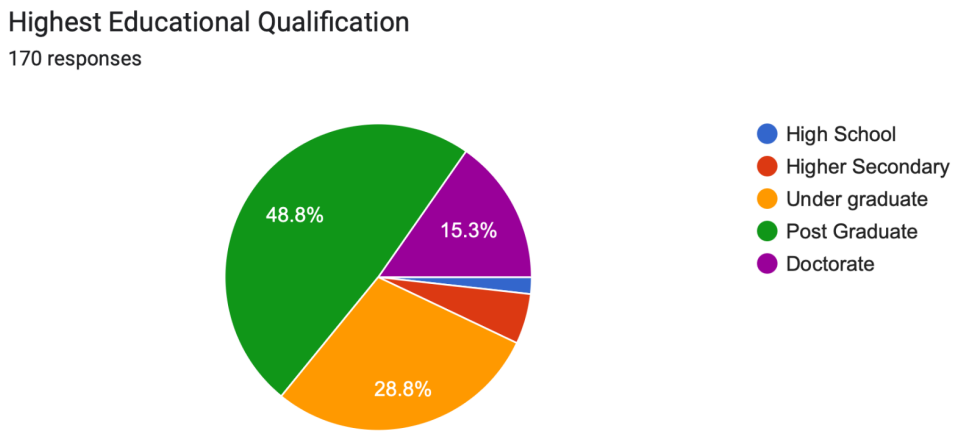
- 'Student' emerged as the dominant occupation among the respondents. This aligns with the age distribution of the sample population.
- Other subgroups within the population include working professionals, self-employed individuals, a few homemakers and retired individuals.
- The diversity in occupation, though student-heavy, still includes those who are financially independent and likely to make independent online purchase decisions.

Implications:

- The dominance of students means the dataset may reflect values *such as heightened awareness of data privacy, but potentially less risk aversion due to lower financial stakes*.
- The presence of working professionals adds more balance. This is so because they

would be more conscious of the risks of online personal data sharing because they have more at stake.

Highest Educational Qualification



- A substantial majority of respondents hold a graduate or postgraduate degree, suggesting a sample that is well-educated.
- A smaller portion includes respondents with school-level education or PhDs, indicating variance in educational attainment.

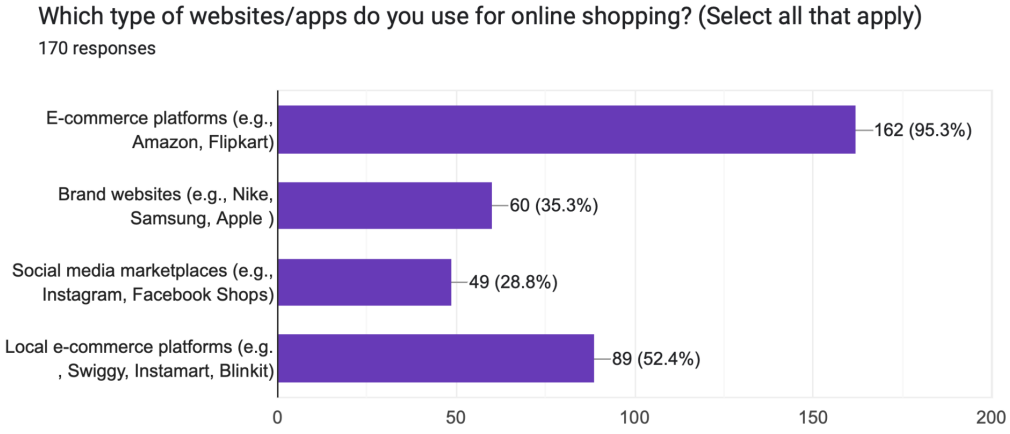
Implications:

- The respondents are likely to be aware of privacy-related issues, read or at least be aware of privacy policies, compliance standards, and data protection laws, making their responses of the population particularly valuable.

In conclusion, the demographic section reveals that the sample is primarily composed of young, urban, educated individuals. Many of the respondents are students or working professionals. This aligns well with the focus of the study on urban online shoppers. However, owing to the nature of the sample, it might skew slightly more toward digitally literate and possibly privacy-conscious users.

Factors Influencing Consumers' Willingness to Share Personal Data

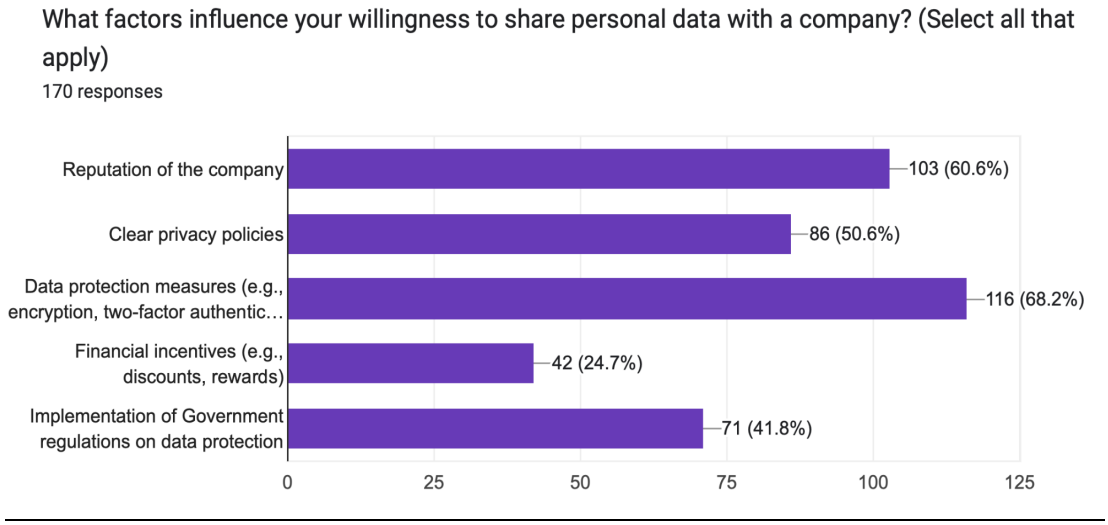
This subsection explores the key elements/factors that shape a consumer's willingness to share personal data. It analyses the types of personal data users are willing to share and consequently the conditions under which they are willing to do the same.



- The most commonly selected platforms are likely major players like Amazon, Flipkart, and possibly other Indian or international e-commerce apps.
- Since respondents could select multiple platforms, this shows that consumers often use a variety of apps, indicating multi-platform engagement.

Implications:

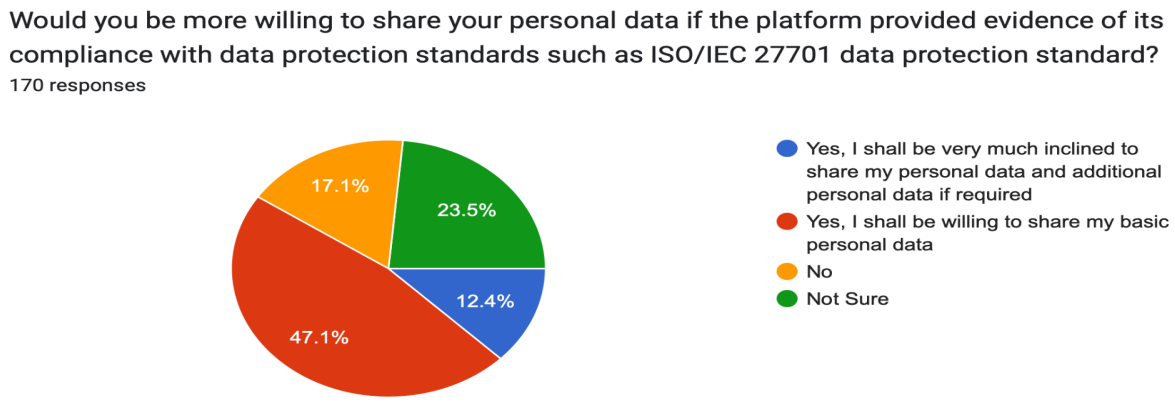
- From the interpretation of the data, it can be said that the consumers are 'platform-fluid'. This means that they will shift their loyalty if one platform offers better trust signals (like stronger data protection or more transparent policies). The biggest determinant for a consumer to choose a particular platform over other similar competing platforms could be factors such as price and quality. However, keeping other factors the same, the lack of security of personal data can be a deal breaker.



- Key factors influencing the respondents' willingness to share personal data included strong data protection measures, reputation of the company and visible compliance with data protection laws & regulations (such as GDPR & DPDPA).
- Data protection measures emerged as the main factor influencing consumers' willingness to share personal data. Surprisingly, financial incentives didn't play a huge role.

Implications:

- This is strong evidence for business organisations to implement strong data protection measures such as encryption & two-factor authentication to get a strategic advantage over their competitors.
- Consumers valued the implementation of government regulations much less than data protection measures. This could be because the respondents do not trust the efficacy of the state in implementing data privacy laws properly or the law enforcement mechanism of the country in general.
- Consumers are highly concerned about their personal data, and even financial incentives are not significantly motivating them to share it. While financial gain is typically a strong driver of behaviour, in this context, it appears insufficient to override privacy concerns.



- 59.5 % of the respondents stated that they would be willing to share personal data, with 12.4% stating that they would be willing to share *additional personal data* if the organisation showed visible proof of compliance with international standards of data protection.
- Only 17.1% of the respondents gave a clear 'No'

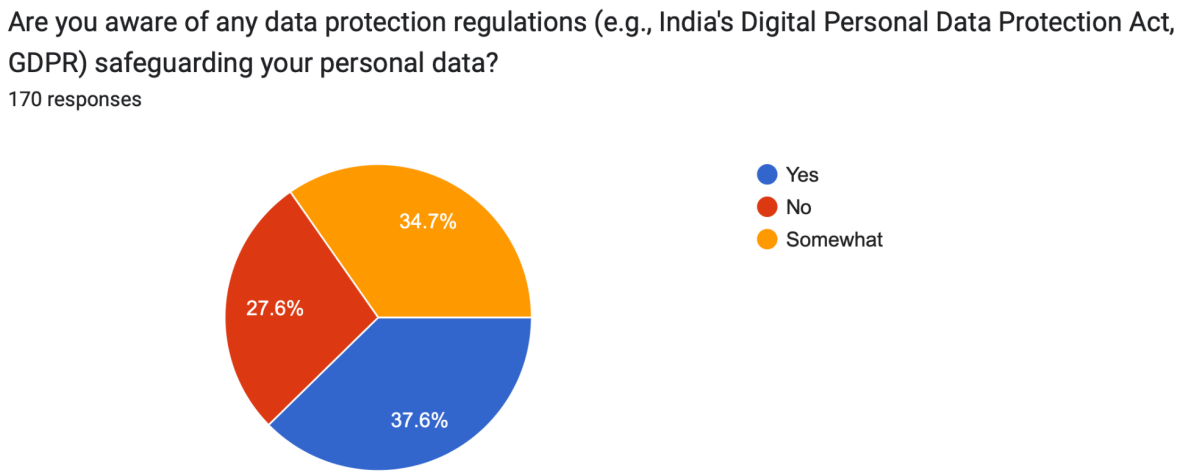
Implications:

- 23.5 % of respondents marking 'Not Sure' could be potentially because they are not aware of what these data protection standards are, such as the ISO/IEC 27701.
- 17.1 % of respondents marking 'No' could be because they do not trust the effectiveness of the ISO standards themselves.
- Marketing trust becomes just as important as building it. Consumers need to see the proof, not just promises.

In summary, this section reveals that:

- Consumers shop across multiple platforms but are cautious with personal data. They can be platform fluid.
- The most powerful influencers of data-sharing behaviour are data protection measures such as encryption, two-factor authentication, etc. Compliance with data protection laws and regulations proves inadequate for consumers to freely share personal data.
- Consumers are more willing to share personal data with demonstrable and visible efforts toward privacy compliance and protection, such as ISO certifications.

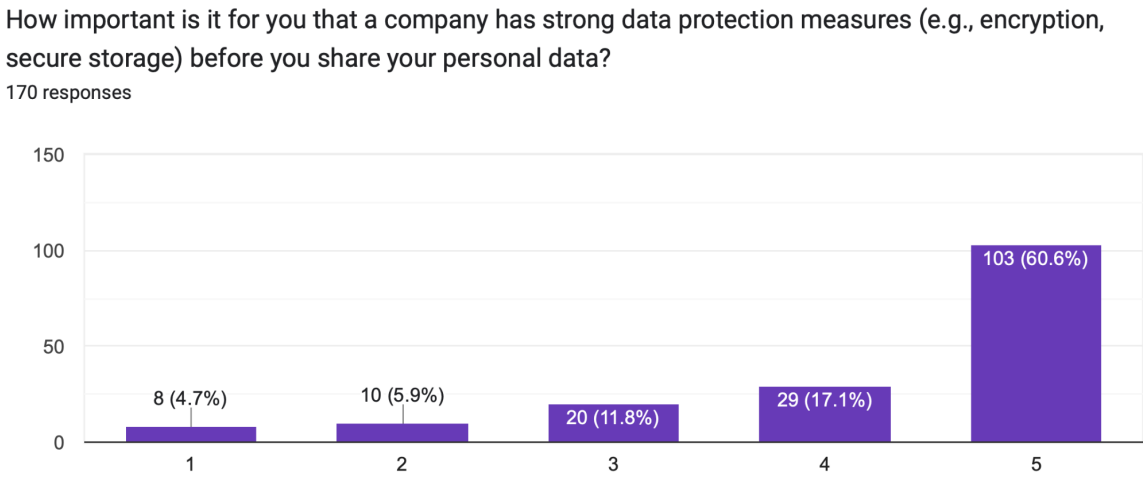
Data Protection Measures and Consumer Data



- 27.6% of the respondents only said that they didn't know about any protection regulations/legislation.
- 72.4% of the respondents were either partially or fully aware of such regulations/legislations.

Implications:

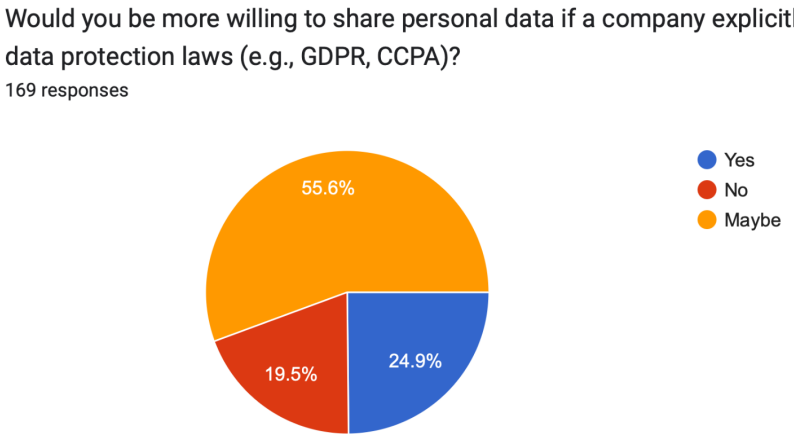
- Awareness of regulations is present but not universal. General Awareness about data privacy regulations could be because of the fact that this sample was an educated sample.
- The government needs to educate consumers more explicitly about their data protection rights.



- A majority with 77.7% responded with “Very important” or “Important”,
- Very few may have chosen “Not important”.

Implications:

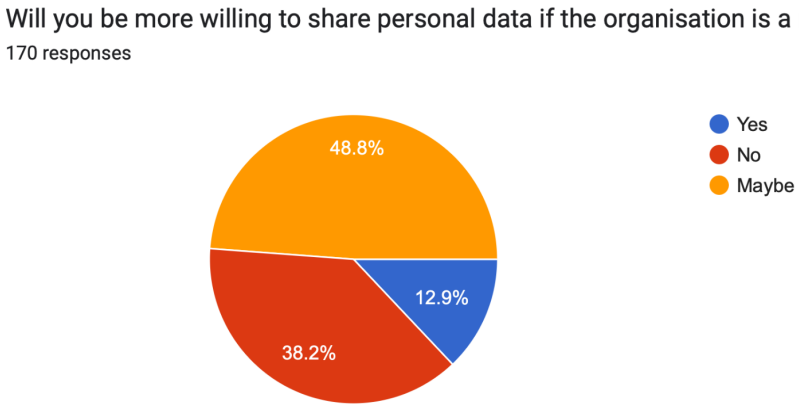
- This proves that data protection is not a compliance burden but rather a strategic imperative.
- Encryption, secure data storage, and third-party restriction policies are the most effective trust-building, privacy-preserving measures.
- Since they are considered very important and held highly by consumers, companies should clearly communicate the initiatives that they undertake to preserve personal data. Businesses should highlight these features clearly and not bury them in T&Cs or legalese.



- The vast majority are expected to have selected "Yes", but surprisingly, only 24.9% of respondents have only marked 'Yes '

Implications:

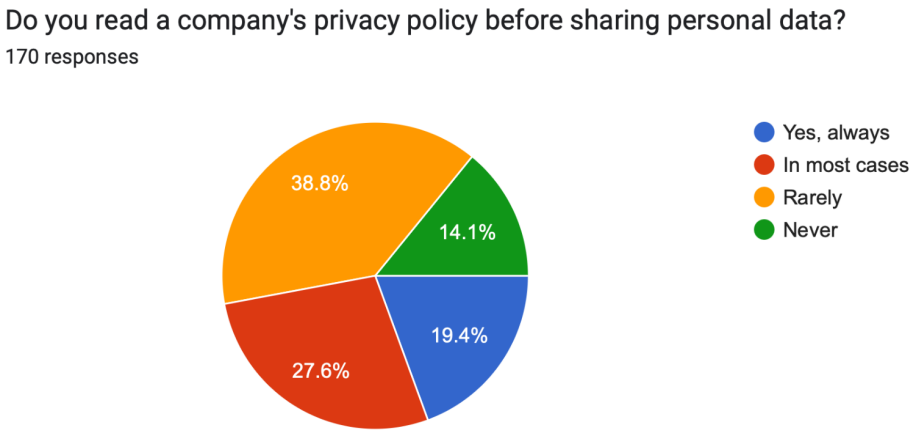
- 75.1% responded either 'Maybe' or 'No'. This result could either be interpreted as a lack of general awareness by the respondents about privacy regulations or deep-seated mistrust in the efficacy of established legal mechanisms in India and abroad.
- Consumers might need tangible proof, such as audits, to come to the personal conclusions that their personal data is actually protected by these e-commerce companies. Claims without solid, trustworthy evidence would be inadequate to gain consumer trust.



- Only 12.9% of consumers trusted MNCs.

Implications:

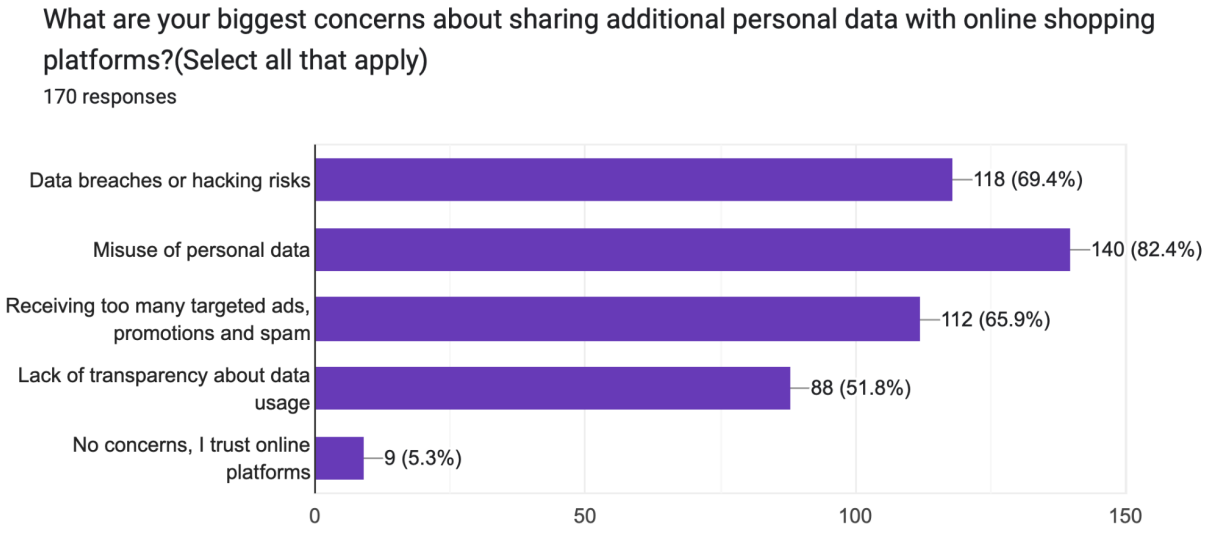
- One possible explanation for this could be that consumers see MNCs as exploitative. They might feel that MNCs feed on their personal data to further their greedy business interests. They may perceive them as faceless, profit-driven entities. They could also be sceptical of MNCs due to past data misuse scandals that were in the news (e.g., Facebook/Cambridge Analytica), etc.
- The brand image and reputation of a company matter, not just its geographic scope, size and capital.



- More than half of the respondents never or rarely read the privacy policy, while the other half always read privacy policies or in most cases.

Implications:

- There is a major gap between privacy awareness and actual behaviour.
- The researcher doubts the truthfulness of the claim that 48 per cent of the respondents either always read a privacy policy or read a privacy policy in most cases. This can be influenced by respondents' desire to appear knowledgeable.
- Many may acknowledge the length and complexity of these documents as barriers.
- Companies should consider simplifying privacy policies and offering "key point summaries" and visual explanations.



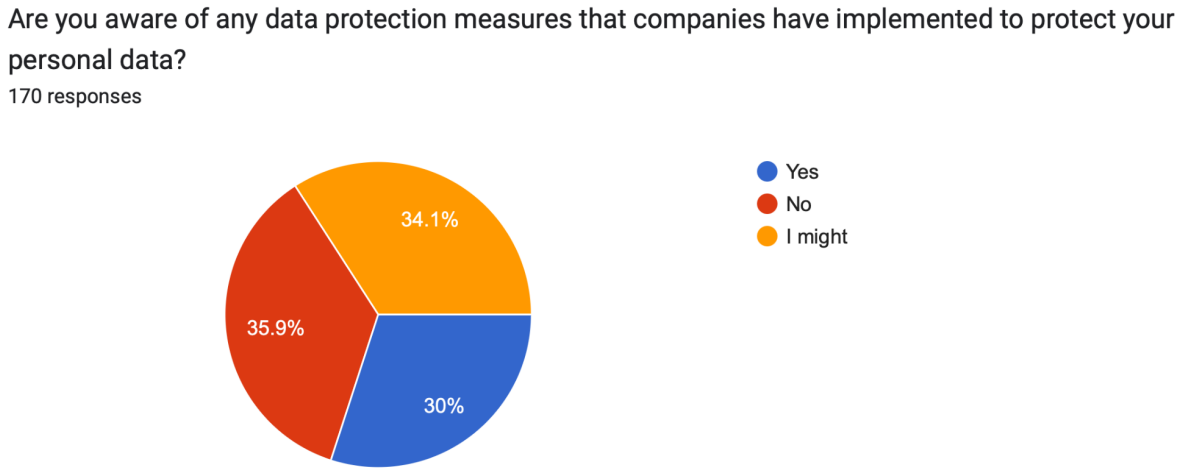
- Misuse of personal data emerged as the biggest concern. Misuse of personal data refers to the unauthorised, unethical, or illegal collection, processing, sharing, or handling of an individual's personal data.
- Data breaches and hacking, closely followed by receiving targeted ads, were among the main concerns that respondents pointed out.

Implications:

- Consumer fears are both technical (security flaws) and ethical (misuse, overreach).
- Addressing both requires a combination of technical systems (encryption, access logs) and ethical design principles (purpose limitation, role-based access control).

Effectiveness of Data Protection Measures in Building Consumer Trust

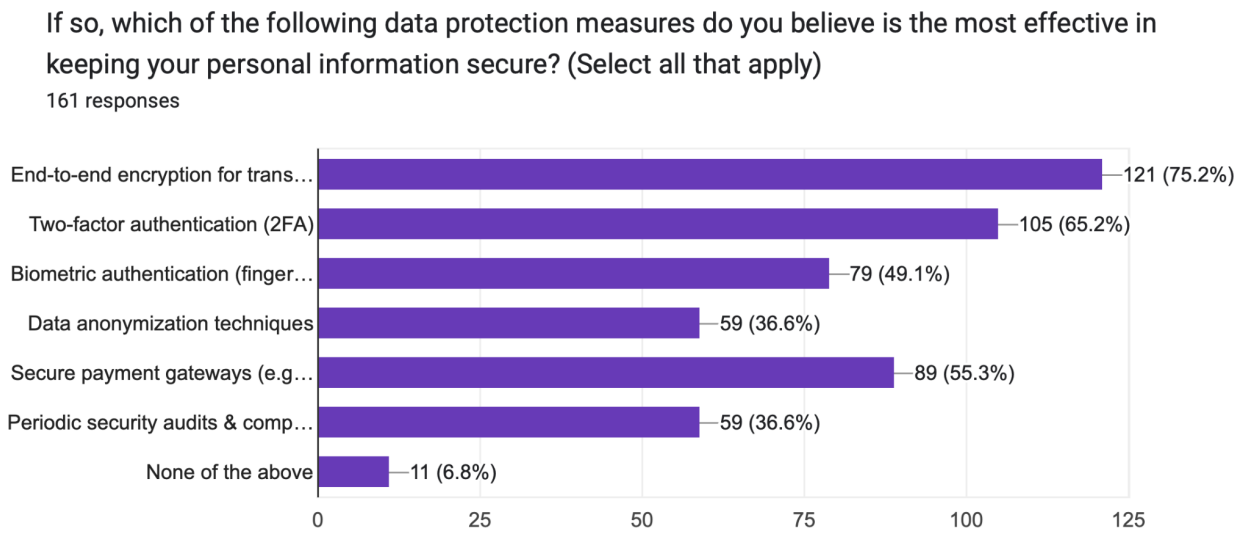
This section explores how effective data protection measures not only safeguard personal information but also foster a sense of security and trust among consumers.



- Only 30% of users are actively aware of the data protection measures that companies have implemented to protect their data.
- 70% of respondents may have selected “No” or “I might,”

Implications:

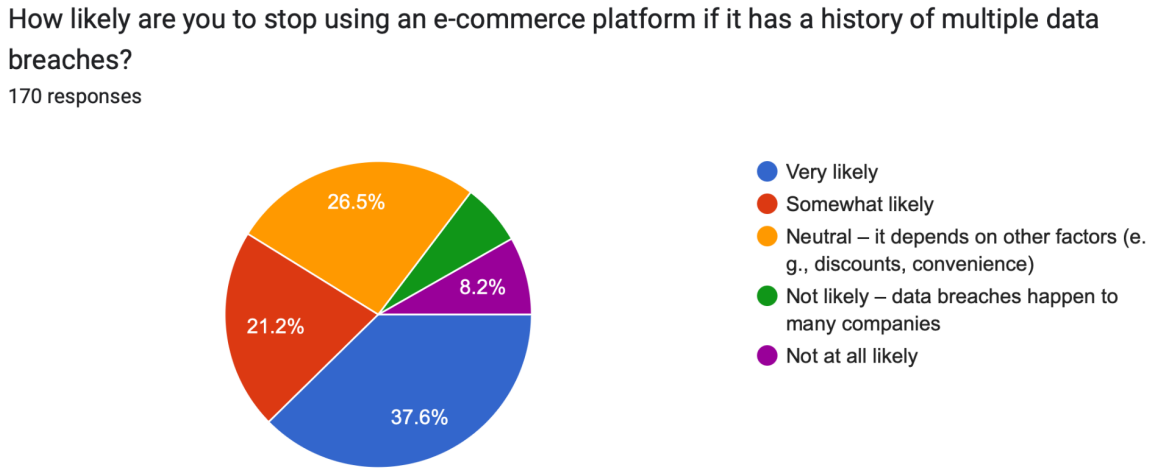
- Many consumers are at least vaguely aware of data protection practices, though the level of technical understanding might vary. This can also indicate that not all companies clearly communicate the security steps they undertake to their consumers.
- This suggests the need for companies to do more to advertise and inform users, ideally within the user interface (e.g., pop-ups during login, privacy notifications), about the privacy-preserving technologies and other safeguards that they provide.



- Common selections likely include:
    - End-to-end encryption of data
    - Two-factor authentication (2FA)
    - Secure servers / secure socket layers (SSL)
    - Biometric authentication

Implications:

- Consumers clearly prioritise technical security practices like encryption and two-factor authentication (2FA) over other privacy-preserving technologies. This could be because the existence of these technologies is common knowledge to consumers.
- Even if they don't fully understand the back-end mechanisms, they associate these terms with safety and modernity.



- 58.8% of respondents marked either "Very likely" or "Likely".

Implications:

- Breaches break trust, and repeated breaches make brand recovery extremely difficult. Data breaches affect brand loyalty.
- A small group might indicate "Unlikely," most possibly because of lack of alternatives, product reliance, or perceived inevitability of breaches.

In conclusion, this section demonstrates that

- The respondents are not very well aware of data privacy laws & regulations.
- Encryption, secure payments, and two-factor authentication emerged as the most sought-after data security measures, which respondents believed protected their personal data.
- Consumers are willing to abandon platforms that fail to protect their personal data and suffer frequent data breaches.

LIMITATIONS OF THE STUDY

This study is not without its limitations. These limitations should be acknowledged to ensure transparency and to contextualise the scope and applicability of the findings.

Sampling Bias

- The study utilised a non-probability convenience sampling method. The sample questionnaire was primarily disseminated through online platforms and social media. As a result, the sample may not be fully representative of the broader population of online shoppers in urban India.
- The sample skewed heavily towards students and younger adults (18-30 years), many of whom were currently pursuing or had completed higher education. *This may have introduced an education and digital literacy bias. This limits the generalisability of the results to older or less digitally engaged populations.*

Geographical and Socioeconomic Concentration

- Although the study focused on urban India, the respondents were not evenly distributed across different Indian cities or socioeconomic strata of urban India. The respondents were mostly from cities in the states of West Bengal and Kerala, such as Kolkata, Kochi and Thiruvananthapuram.

- *The sample leaned toward middle-class, educated individuals with regular access to the Internet and digital payment systems.*

Self-Reported Data

- All findings are based on self-reported responses, which are subject to social desirability bias and recall bias.
- Participants may have overestimated their awareness of privacy laws or their trust in platforms, or may have misunderstood the technical nature of some questions (e.g., encryption, ISO/IEC standards).

Lack of Longitudinal or Experimental Design

- This study was cross-sectional and conducted within a limited time frame. It captures attitudes and behaviours at a single point in time. It does not assess how consumer trust or behaviour may change over time. A longitudinal or experimental design could have yielded better causal insights.
- This study, therefore, has to be viewed and interpreted keeping in mind the lack of

long-term observation, which is a crucial requirement in arriving at conclusions in studies of this nature.

Exclusion of Qualitative Analysis

A full thematic analysis of qualitative data was not performed. Future research could benefit from a mixed-methods approach. This can include detailed interviews or focus groups to gain richer, more nuanced insights into consumer perceptions.

SUMMARY OF FINDINGS

The following are the major findings of the study:

1. Demographics and Digital Literacy

- The demographic profile of respondents was skewed toward young, educated individuals. This aligns well with the broader market trends of younger, digitally literate populations being the primary drivers of e-commerce adoption in India[27].
- The implications of this particular demographic composition are twofold. On the one hand, respondents demonstrated a relatively high level of awareness regarding privacy issues and compliance standards. On the other hand, the dominance of students, who may face lower financial risks, suggests that their attitudes toward data sharing could reflect a degree of experimentation or reduced risk aversion. By contrast, working professionals could be more cautious, as their financial independence and exposure to workplace digital systems likely sharpened their sensitivity to privacy risks.

2. Platform Usage and Consumer Behaviour

- The findings indicate that urban Indian consumers are platform-fluid as they engage with the usage of multiple e-commerce websites and applications simultaneously for shopping, such as Amazon, Flipkart, etc.
- This shows that they are inclined to switch between platforms depending on factors they deem appropriate. Trust signals can be one of the decisive factors.

[27] CNBCTV18, "Gen Z fastest growing demographic to adopt e-commerce: Meesho", *CNBCTV18*, *available at*: https://www.cnbctv18.com/travel/lifestyle/gen-z-fastest-growing-demographic-to-adopt-e-commerce-meesho-19456680.htm (last visited on: Aug. 16, 2025).

- This finding underscores the strategic value for e-commerce businesses of integrating strong privacy safeguards into their consumer proposition. In an environment where switching costs for users are minimal, the ability to communicate trustworthiness becomes a powerful differentiator.

3. Determinants of Willingness to Share Personal Data

- The survey results confirmed that strong data protection measures such as encryption, two-factor authentication(2FA), and secure data storage techniques and technologies are the leading data privacy measures to build trust with consumers. Compliance with data protection laws or financial incentives weren't marked as the leading factors.

- Providing evidence of compliance with international standards of data protection, such as ISO/IEC 27701, was also found to have a substantial impact. Nearly 60% of respondents reported that they would be more willing to share personal data if visible proof of compliance with such standards was provided. At the same time, a quarter of the respondents stated that they were unsure whether the implementation of international standards was effective in safeguarding their personal data.

- Notably, financial incentives did not exert a significant influence on consumers' data-sharing decisions. While discounts and personalised services remain attractive, they were insufficient to override privacy concerns. This finding challenges common industry assumptions that monetary benefits can offset consumer anxieties about privacy.

4. Trust in Regulations versus Certifications

- A striking theme emerging from the study is the *differential trust placed in regulations and certifications*. While most respondents were aware of data protection laws such as the GDPR and India's Digital Personal Data Protection Act (DPDPA), they expressed limited confidence in regulatory enforcement mechanisms.

- Only about a quarter indicated that explicit claims of legal compliance would increase their willingness to share data, whereas more than half adopted a cautious "maybe" stance. This reflects a broader scepticism about the state's ability to monitor violations, penalise non-compliance, and safeguard individual rights effectively.

- By contrast, respondents demonstrated greater confidence in *auditable, standardised certifications* and visible technical safeguards such as ISO certifications, 2FA, end-to-end encryption, etc. The respondents see institutional enforcement as weak, while independent certifications are seen as credible.
- It may also be inferred that respondents' scepticism of legal compliance as a method for protecting their personal data could stem from a perception that Indian law enforcement mechanisms are insufficient to disincentivise corporate misconduct. The respondents may compare to foreign jurisdictions where law enforcement is viewed as stricter and less susceptible to corruption or inconsistency.

5. Trust in Multinational Corporations (MNCs)

- Only 12.9% of respondents indicated a higher trust in MNCs, possibly due to their size and capital.
- The reason for such low trust in MNCs, even though they have the capital to implement data protection standards, could be that many participants may perceive MNCs as exploitative and profit-driven entities.
- The results imply that brand reputation and ethical track record matter more than geographic scope. In fact, the foreign origin of a platform was not seen as a guarantee of stronger privacy practices.

6. Engagement with Privacy Policies

- A persistent gap emerged between privacy awareness and behavioural engagement. While respondents acknowledged the importance of privacy protections, more than half admitted they rarely or never read privacy policies. This behaviour highlights the well-documented phenomenon of "consent fatigue", wherein consumers are overwhelmed by lengthy, complex legal documents, which results in them technically consenting to processing that is against their best interest [28].
- Even among those respondents who claim to read privacy policies sometimes are

[28] Secure Privacy, "Adaptive consent frequency: Using AI to combat consent fatigue", *available at*: https://secureprivacy.ai/blog/adaptive-consent-frequency-using-ai-to-combat-consent-fatigue (last visited on Aug. 16, 2025).

almost always, the responses may have been influenced by social desirability, with participants overstating their diligence.

- The implication is that companies cannot rely on traditional, legalistic privacy policies to communicate their privacy practices and consequently build trust. Instead, they should invest in simplified, accessible, and user-friendly privacy communications.

7. Concerns About Data Sharing

- The respondents marked misuse of personal data as their biggest concern. Misuse in this context can mean the unauthorised use and exploitation of consumers' personal data by the corporation without their informed consent.
- The concerns of the respondents may range from technical issues, such as weak security systems, to ethical concerns, such as their personal data being unethically exploited to generate profits.

8. Effectiveness of Data Protection Measures

- The findings also suggest that awareness of data protection measures is limited.
- Only about 30% of respondents were actively aware of the specific privacy safeguards implemented by companies. This points to a communication deficit. Companies may have adopted advanced practices, but they are not clearly advertising them to users.
- Nevertheless, when asked which measures they perceived as most effective, respondents consistently prioritised end-to-end encryption, secure servers, and two-factor authentication. These technologies have become widely recognised by consumers as reliable markers of safety.
- Another key finding is that repeated data breaches severely undermine consumer trust and brand loyalty. Nearly 60% responded that they would be very likely or likely to abandon platforms with a history of multiple breaches. This demonstrates that privacy failures carry long-term reputational costs that are difficult to repair, regardless of subsequent improvements in security.

In sum, the findings strongly support the central hypothesis of this study that urban Indian consumers are more willing to share personal data with e-commerce platforms when those platforms provide visible and credible evidence of compliance with data protection standards.

The notable finding in the study, however, is that the *consumers prefer certifications, use of privacy-preserving technologies and other similar indicators over a claim or proof of compliance* with data privacy laws & regulations. Consumers value tangibility. Therefore, *the hypothesis is irrefutably proven based on the data and analysis conducted.*

CONCLUSION

Therefore, the overarching conclusion of this study is that '*trust is the most valuable currency'.* While scepticism toward regulatory enforcement persists, certifications and technical measures act as credible trust signals. For e-commerce platforms, building long-term consumer trust requires moving beyond symbolic compliance to demonstrable privacy-preserving practices. Organisations reap long-term benefits in the form of increased engagement and brand loyalty from implementing privacy-preserving practices.