# Major Research Project

## SILENT SURVEILLANCE:

## HOW PERSONALIZED DIGITAL MARKETING INVADES CONSUMER PRIVACY IN INDIA

*A Study of Consumer Awareness, Attitudes, and the Path to Ethical Marketing*


Submitted By

**Mridul Jain**

**24/DMBA/142**

MBA — Delhi School of Management

Under the Guidance of

**Dr. Yashdeep Singh**

**Assistant Professor, DSM, DTU**

**DELHI SCHOOL OF MANAGEMENT**

**Delhi Technological University**

**Bawana Road, Delhi – 110042**


Session: 2024 – 2026

# CERTIFICATE

This is to certify that the Major Research Project entitled "SILENT SURVEILLANCE: HOW PERSONALIZED DIGITAL MARKETING INVADES CONSUMER PRIVACY IN INDIA" submitted by Mridul Jain, 24/DMBA/142 student of MBA programme at Delhi School of Management, Delhi Technological University, in partial fulfilment of the requirement for the award of the degree of Masters in Business Administration during the academic year 2025–26.

Dr Yashdeep Singh

Assistant Professor

Delhi School of Management

Delhi Technological University

Date: _____

# DECLARATION

I, Mridul Jain, Roll No. 24/DMBA/142 a student of MBA hereby declare that the Major Research Project titled "SILENT SURVEILLANCE: HOW PERSONALIZED DIGITAL MARKETING INVADES CONSUMER PRIVACY IN INDIA" submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at Delhi School of Management, Delhi Technological University, is my own original work.

This report is original and has not been submitted, either in whole or in part, to any other institution or university for any award. All the sources and references used in the course of this research have been duly acknowledged. Most of the data presented in this report is taken from the original survey, and the analysis is entirely my own.

I further confirm that this report is compliant with the plagiarism policy of Delhi School of Management and the similarity index is less than the prescribed limit of 20 percent.

Mridul Jain
MBA, Delhi School of Management
Delhi Technological University

Date: _____

# ACKNOWLEDGEMENT

It has been an enriching experience for me to be able to successfully complete this Major Research Project and I believe that I could never have done it without the assistance of certain individuals whose contribution I would like to acknowledge from the depths of my heart.

First of all, I want to thank my guide Dr. Yashdeep Singh, Assistant Professor, Delhi School of Management, DTU for her immense guidance in preparing this Major Research Project. She provided me with excellent feedback. I deeply value her contribution and the guidance she provided me with in completing this Major Research Project.

Next, I would like to express my gratitude towards the Head of the Department, Dr. Saurabh Agarwal of Delhi School of Management. He ensured that I had everything I required in order to undertake my Major Research Project. He made my work easier by supporting me at all times and encouraging me which served as a big source of motivation to me. My family and friends too greatly contributed in helping me accomplish this task by supporting me wholeheartedly.

Last but not the least, I would like to thank the Delhi Technological University for giving me this opportunity to conduct this Major Research Project as a part of my MBA course. The Major Research Project has been of great help to me in increasing my knowledge on the subject of marketing which is my specialization area.



Mridul Jain

Delhi School of Management

Delhi Technological University

# EXECUTIVE SUMMARY

India's digital penetration is growing faster than other markets around the world and has already reached scale, with almost one billion internet connections, and millions of users added every month. At the heart of this development is a business model based on the idea of 'free services for personal data'. Platforms use behavioural data to turn every use of the search, or every use of an app, or every map query into advertising dollars. Although there are many who do it willingly, most users are not aware of what information is being collected, who is responsible for it, or if they are actually being given the choice to consent.

The gap is found in this Major Research Project "Silent Surveillance: How Personalized Digital Marketing Invades Consumer Privacy in India". A structured primary survey was conducted on a sample of 192 respondents, primarily young adults aged 18-30, who were interviewed to explore the levels of awareness and emotional responses to data tracking, actual privacy protection behaviors, and attitudes towards personalization in a transparent context.

Descriptive analysis, Pearson correlation (H1 and H4), Chi-Square test of independence (H2), one-way ANOVA (H3), independent-samples t-test, and Cronbach's Alpha reliability analysis were used to analyse the data. Three composite indices have been created: Awareness Index, Privacy Concern Index and Personalization Acceptance Index.

The study yielded some important results. First, 92.7% of respondents reported having seen a targeted ad for something they just talked about recently and then never searched out online – the “phone listening” phenomenon. Second, 74.5 per cent of respondents confessed to providing false personal information in applications at least sometimes to ensure privacy protection, which has not been extensively explored in the Indian research literature. Third, the results of the present study supported Hypothesis 1: awareness of data tracking is positively and significantly related to privacy concern ($r = 0.322$, $p < 0.001$). All three other hypotheses were not supported with each having its own implication: privacy policy neglect is a cross-sectional

phenomenon across occupations, privacy concern is a cross-sectional phenomenon across age groups, and concern is not predictive of willingness to pay for privacy-preserving products—a confirmation of the Privacy Paradox in the Indian context.

Finally, the report proposes six recommendations for good marketing practices: contextual advertising, first-party data strategies, zero-party data collection, transparent consent architecture, Privacy by Design, and enforcement of the Digital Personal Data Protection Act 2023. The key idea is that privacy issue cannot be solved by market mechanisms, but needs structural regulatory measures.

# TABLE OF CONTENTS


| Section | Page No. |
|---|---|
| Executive Summary | iii |
| **Chapter 1 — Introduction** | 1 |
| 1.1 Background | 1 |
| 1.2 Problem Statement | 3 |
| 1.3 Objectives of the Study | 4 |
| 1.4 Scope of Study | 5 |
| **Chapter 2 — Literature Review** | 7 |
| 2.1 Surveillance Capitalism | 7 |
| 2.2 Data Collection Mechanisms | 8 |
| 2.3 The Privacy Paradox | 10 |
| 2.4 Indian Consumer Awareness | 11 |
| 2.5 Consequences of Privacy Invasion | 12 |
| 2.6 Ethical Marketing Frameworks | 13 |
| **Chapter 3 — Research Methodology** | 15 |
| 3.1 Research Design | 15 |
| 3.2 Sampling | 16 |
| 3.3 Data Collection Instrument | 16 |
| 3.4 Hypotheses | 17 |
| 3.5 Analytical Techniques | 18 |
| 3.6 Limitations of the Study | 19 |
| **Chapter 4 — Analysis, Discussion and Findings** | 20 |
| 4.1 Respondent Profile | 20 |
| 4.2 Awareness of Data Tracking | 24 |
| 4.3 Emotional Response to Targeted Advertising | 27 |
| 4.4 Composite Index Analysis | 29 |
| 4.5 Hypothesis Testing | 31 |

| Section | Page No. |
|---|---|
| 4.6 Behavioral Insights | 39 |
| 4.7 Personalization and Privacy Trade-Off | 43 |
| 4.8 Benchmark Comparison | 45 |
| **Chapter 5 — Conclusions and Recommendations** | 47 |
| 5.1 Summary of Conclusions | 47 |
| 5.2 Recommendations | 49 |
| 5.3 Final Reflection | 52 |
| **References** | 54 |
| **Annexure — Survey Questionnaire** | 57 |

# CHAPTER 1: INTRODUCTION

Hundreds of millions of India users are logging into Instagram, searching Google, ordering food on Zomato and chatting on WhatsApp and with everyone, each day, and with each of these interactions, they leave behind behavioural data. That information is gathered, deciphered, compiled, and sold to advertisers who use it to display exactly targeted ads to exactly targeted consumer groups. For the advertiser it is efficient marketing. To the consumer, it may seem like a completely different experience.

This research project is driven by a question which almost every Indian smartphone user asked at some point in their lives: why did I see that ad? Not a general ad, but a specific one — one for the product you just spoke with a friend about, one for the restaurant in the city you're considering for vacation, one for the medicine you're a friend of someone in your household was studying. It's a common occurrence and has become a colloquial term: "phone listening. Yes, the technical explanation of what is happening is more complicated than accessing microphones, but the truth is that social platforms have more information about their users than their users have purposefully given them.

This study explores that disconnect between what digital platforms take and what the Indian consumers know, feel and do about it. It's a study on awareness, attitude and behavior at a time when India had its first comprehensive data protection law, but has not yet started enforcing it.

## 1.1 Background

Digital India is one of the fastest growing new areas of India's development in the last 10 years. By 2024, there were an estimated 10 million monthly new internet connection users and around 96.96 crore internet connections in the country (NITI Aayog, 2024). Social media, e-commerce, food delivery, navigation, entertainment — the sites where much of this digital interaction takes place — run under a business model whose basic tenets are the trade of free service for personal data.

In this model, platforms are not just gathering data that is required to deliver their services, but also data that is not. In the best terms they can be described as surveillance capitalism, as portrayed in the best terms by the economist Shoshana Zuboff. They gather as much as they can: their browsing history and their purchase history, their

location and their social circles, how they feel and their behavioral patterns, so they can create more and more accurate models of what they are doing right now and what they will be doing in the future. These models are then offered, as targeted advertising inventory, to brands which wish to target specific consumers at moments of high purchase intent.

This is a big infrastructure in India. Instagram (93.2 per cent), WhatsApp (90.6 per cent) and YouTube (76.6 per cent) are all based on this model, and are the most popular apps used by respondents to this study. Each of these applications keeps more information than may be needed to provide the service, and many share information with or sell it to third parties, which is disclosed to consumers in terms of privacy policies that most people don't fully grasp.

Meanwhile, the preference of outcomes of this data gathering customises recommendations, advertisements, and content is high. The 2025 study by Qualtrics XM Institute, which polled 23,000 consumers in several countries found that the Indian consumers were the largest in choosing to interact with a brand that caters to their tastes, with 82 per cent favouring such personalised interactions. The core contradiction studied in this research is that consumers desire personalization, but the process whereby that is achieved is a process they are not familiar with and once they do understand, they are not very fond of.

This moment is made urgent by the regulatory context. The first comprehensive legislation on personal data protection was enacted in India in 2023, the Digital Personal Data Protection Act (DPDP Act). The Act requires specific informed consent for each type of data that is collected; it provides consumers the right to know what data is being retained about them, the right to correct and the right to have the data erased. Penalties for violations are up to Rs. 250 crore per contravention. At the time of this research, there were no enforcement mechanisms in place, and they remain in law but not in practice.

## 1.2 Problem Statement

This study seeks to address the structural disconnection between the processing of consumer information by digital marketing platforms and what the Indian consumer,

in particular young educated digitally active adults, knows and understands about their processing of the consumer information.

This gap exists on three levels. The first is awareness: Most consumers are unaware of the data collected, how it's collected, by whom, and for what. ComplyZero, which conducted the audit of more than 6000 Indian websites this year, found that 95.9 per cent of these collected user information without their consent using tracking technologies. According to a consumer survey conducted by PwC India in 2024, just 16 per cent of the respondents in India were aware of the DPDP Act and 56 per cent had no knowledge about their rights regarding data.

Consequence is the second level, as the consequences of data practices of digital marketing platforms are real harms for consumers: financial harms, psychological harms (chilling effect of perceived surveillance), identity-related harms (data breaches), and autonomy harms (algorithm manipulation of preferences, choices).

Solution: The current consumer discussion about digital privacy emphasises consumer education as the key solution. But the evidence just doesn't back that up, this study suggests (as awareness, even if linked to concern, does not lead to changes in behaviour as consumer education campaigns do assume). The Privacy Paradox, the documented discrepancy between concern and protective behavior, is no joke and solutions need to take it into consideration.

## 1.3 Objectives of the Study

This research project aims to achieve four goals:

To understand the awareness of the Indian youth on the collection, usage, and sharing of their personal data with digital marketing platforms.

To measure the emotional and attitudinal reaction of consumers to targeted advertising and data tracking, and to find out if transparency in data practices affects consumer trust.

To capture and study the behavioral reactions of Indian consumers towards the privacy concerns in both formal and informal ways.

To find and suggest ethical marketing solutions that enable brands to personalize communications without sacrificing the use of surveillance data.

## 1.4 Scope of Study

This study is limited to urban India, mainly the metropolitan cities of Delhi NCR. The target is young adults (18-30 years) and there is a strong presence of post-graduate students and early career professionals. This group was selected due to its heavy usage of the digital platforms that will be studied, in addition to being the demographic group that directly falls within the reach of data-driven marketing throughout the years in which brand preferences and consumption habits are formed.

The study includes practices of consumer-facing digital platforms for social media, e-commerce, food delivery, and search, but it will not cover business-to-business practices, government data collection, or offline marketing practices. The survey was obtained by a structured online survey that was conducted by Google Forms from April to May 2026, with 192 valid responses.

The study is of cross sectional type and descriptive analytical. It does not make causal claims, but seek to establish links, test hypotheses and draw conclusions that can be used to make policy decisions on consumers and brands in the context of the existing regulatory framework in India.

# CHAPTER 2: LITERATURE REVIEW

The purpose of this chapter is to summarize the academic and empirical literature that is relevant to the four research objectives of this study. The review is broken down into six thematic sections, starting with the theoretical foundations, documented mechanisms, established empirical findings, consequences, and emerging ethical frameworks.

## 2.1 Theoretical foundations of Surveillance Capitalism. Theoretical framework of Surveillance Capitalism.

Zuboff's (2019) "surveillance capitalism" is the most significant theoretical approach to understanding digital marketing data practice. Zuboff proposed that the prevailing internet companies of the twenty-first century have grown a new twenty-first century economic logic, using human behavioural experience, the stuff of consciousness, choice and social life, as the raw material of a production line that produces prediction products. This is because these prediction products are sold to advertisers who are not just trying to get customers' attention, but influence their behavior.

According to this system, the collection of data is not incidental to the provision of a digital service, but the service itself. The service is the way the behavioural surplus is taken and the product is the prediction. The same analysis Zuboff had applied to Google and Facebook can be used for the Indian platforms in this study. The majority of the respondents in this study (95%, 88% and 94% respectively) use Instagram, YouTube and WhatsApp, which are all based on a variant of the surveillance capitalism model.

Davis and Patterson (2012) expanded on the ethical concerns about data-driven marketing, noting five kinds of harm to consumers: financial harm (from dynamic pricing), psychological harm (feeling watched by the algorithms), identity harm (from data breaches), autonomy harm (from algorithm manipulation), and social harm (the loss of shared norms of privacy). Subsequent studies reviewed in Section 2.5 document each of these harms in the Indian context.

## 2.2 Consumer Data is really collected

With the introduction of the smartphone, the technical literature on what sort of mechanism can be used to collect data has grown immensely. This is why it is important to have an understanding of these mechanisms before interpreting consumer awareness findings.

The oldest and most common is third-party cookies and tracking pixels. A third party will be able to track a user as they visit a website that contains third party cookies, and then follow them through the other websites that contain the same code. According to a systematic review done by PubMed Central in 2024, 62 per cent of the total digital advertising expenditure in the world was driven by this mechanism.

Another more recent and more resistant mechanism is device fingerprinting. It determines a particular device based on the combination of browser version, operating system, screen resolution, installed fonts, graphics hardware specifications and battery level. Contrary to cookies, device fingerprints can't be deleted by deleting cookies or by switching to incognito mode. The majority of customers are completely oblivious to this procedure.

As part of their technical analysis of 18 popular Indian apps on Android, Kohli, Gupta and Gaur of IIT Jammu (2025) discovered the presence of third party software development kits (SDKs) of major companies like Meta and Google in all five categories of apps that they studied, namely social media, education, entertainment, travel, and shopping. As long as these SDKs are running in a host app, they send data about user behaviour back to the parent platform even if the user isn't using the parent platform's own app. It's not microphone access, but data flows from embedded SDKs that provide a similar targeting effect that was reported by 92.7 per cent of respondents in this study.

Dark patterns in consent design is a systemic issue of privacy controls implementation. Only 4.1 per cent of 6,000 Indian websites presented any working consent mechanism, while the majority deployed asymmetric designs, with a big, prominent "Accept All" option and a "Reject All" button that required multiple screens of navigation, according to a report from ComplyZero for the audit. This is fake consent, literally: the legal form of consent without the substance.

## 2.3 The Privacy Paradox

The Privacy Paradox as one of the most consistently documented phenomena in digital privacy research is the difference between users' awareness or concerns about privacy and their actual privacy practices. In seminal studies to date on the subject, Acquisti and Grossklags (2005) demonstrated, in experimental settings, that consumers who were very concerned about privacy would be willing, in exchange for relatively small incentives, to provide their personal data. The paradox is not illogical, but is associated with nature of cognitive mechanisms: dangers of privacy are more abstract, diffuse, and future; benefits of disclosure are immediate and concrete.

Norberg, Horne, and Horne (2007) noted three factors: cognitive overload (most consumers are overwhelmed with the ability to process all the information in privacy policies), social proof (the greater the number of platforms adopted by their peers, the more natural data sharing becomes), and hyperbolic discounting (consumers systematically underestimate future risks compared to present convenience). The results of this study reflect the three: 47.4 per cent of respondents never or rarely read privacy policies, 92.7 per cent used the same platforms known to track the most invasive data, and 20.8 per cent would pay a “small amount” to not have their data tracked.

India has been found to be a clear case of the Privacy Paradox in the Qualtrics XM Institute's cross-national survey – 82 per cent of Indian respondents said that they wanted more tailored interaction with brands, the highest among all nations, and 76 per cent expressed their concerns on using data in social media. It's the shortest form of the paradox, a powerful desire for the product of surveillance, and a lot of discomfort with the product of surveillance.

## 2.4 The Indian Consumer Awareness scale was used to measure the empirical base-line.Empirical baseline:

PwC India's 2024 Data Privacy Landscape survey is the largest empirical baseline of consumer awareness around privacy in India (754 respondents from 24 cities and 186 organisations). The thrust of its key findings is that there is a large awareness gap, with only 16 per cent of respondents being aware of the DPDP Act 2023; 69 per cent having

no awareness of withdrawing consent that they have given; 56 per cent had no awareness of data rights and 84 per cent of the age group of 18-30 years had no awareness of the Act.

Researchers found that there was a strong negative correlation with awareness of privacy concern and trust in platforms with a score of -0.55, meaning that when participants had a higher score for concern about privacy, they had a lower score for trust in platforms (as shown in study published in the International Journal of Scientific Research in Engineering and Management, 2024, 15 (1), 1-36). It was also agreed that the best approach for restoring consumer trust, particularly for high concern consumers, is to have clear communication regarding the handling of data. In fact, 68 per cent of Indian consumers said that they were more inclined to interact with brands that explicitly shared transparency guidelines, according to the Digital Engagement study conducted by Kantar India in 2024. This is similar to the findings from this research, where as 69.3 per cent of the respondents credited brands towards giving them explicit consent to take in data.

The implications of marketing that intrudes into privacy are covered in this course. The impacts of surveillance-based marketing are at two levels: individual consumer harms and commercial brand harms.

## 2.5 Consequences of Privacy-Invasive Marketing

According to the researchers' description, the "chilling effect on digital behaviour" is that 64 per cent of consumers stated that they found location-based ads creepy in Statista's global consumer survey conducted in 2023, meaning they begin to self-censor their search, avoid some apps or select the wrong information. It has been found that dynamic pricing — one that can show different prices to different consumers based on how they have interacted with a website, before they actually make a purchase — is an example of financial exploitation that is not apparent to the consumer, and has been shown to work on travel and e-commerce sites across India. Based on India-specific information provided by CERT-IN, the number of cyberattacks in 2022 rose by 38 per cent from 2021 and personal data breaches accounted for the maximum percentage of these attacks. There is an obvious link

between data collection through surveillance and exposure to subsequent data breaches because the more data that a platform collects, the greater the exposure to data breaches.

The Ponemon Institute (2024) reveals that "65 per cent of consumers are distrustful of a brand if they experience any data breach." The Vercara Consumer Trust and Risk Report (2025) reveals that 70 per cent of global consumers would give up on the brand they were shopping with if they were breached, with 58 per cent stating that they would never trust that brand again. These bad data security experiences were shared publicly with its reputational multiplier effects being greater than the initial incident, as Zhang, Liu et al. (2022) discovered, 85 per cent of consumers who experienced bad data security did so publicly.

## 2.6 Ethical Marketing: What the Literature Proposes

There are a number of recommendations in the literature for ethical marketing.There are many suggestions in the literature about what is ethical about marketing.
Since 2018, when General Data Protection Regulation (GDPR) was introduced in Europe, the volume of literature on alternative approaches to marketing, without the use of surveillance, has grown significantly.As of 2018, there has been a significant amount of literature published on what alternatives there are to surveillance-based marketing, since the introduction of the General Data Protection Regulation (GDPR) in Europe.

For most of the product categories, contextual advertising (ads for content, not for behaviour) is also found to perform similar to behavioural targeting. Businesses such as DuckDuckGo, GumGum and The Trade Desk have developed viable-contextual advertising businesses that don't involve the collection of personal data. The consumer controls what they share, the sharing is explicit, and the resulting data is more accurate than inferred behavioural profiles because it is self-stated rather than inferred. Cavoukian's seven Privacy by Design principles (2009), now referenced in the DPDP Act 2023, provide the architectural framework for embedding this approach into product development.

Cisco's 2024 Data Privacy Benchmark Study, covering 2,600 security and privacy professionals across 12 countries, found that 95 per cent of businesses reported that privacy investments generate returns exceeding their costs, with an average return of 1.6 times the investment in the form of higher consumer trust, reduced churn, and lower regulatory exposure. The commercial case for ethical marketing is, in other words, already made.

# CHAPTER 3: RESEARCH METHODOLOGY

## 3.1 Research Design

In this research, the type of research that is applied is descriptive-analytical research. The aim was to measure and understand consumers' awareness, attitude and behaviours towards digital data privacy and to investigate the hypothesized relationships between these variables. The cross sectional survey design was considered the best design to meet this objective because it provided a standardized sample of data from a large sample within a limited sample time.

The study was a mix method which was quantitative and qualitative. The quantitative part consists of structured questions with fixed answer categories, likert scale items and multiple choice items which are statistically analysed using inferential statistics. The qualitative part consists of two open-ended questions enabling the participants to express their experiences and views in their own words and then analysed using thematic coding.

## 3.2 Sampling

This was a non-probability (convenience) sample and some snowball sampling. The researcher sent the survey to the participants through WhatsApp groups, LinkedIn contacts, and social media and requested participants to share the survey with their contacts. The decision to adopt this approach was based on the feasibility of the approach in the context of an MBA project and because similar digital privacy studies have been undertaken in the context of India (IJSREM, 2024).

192 samples were collected, with two samples rejected for being incomplete. The target set is achieved, as 83.9% of the respondents belong to metros, 53.6% belong to age group between 22-25 and 47.9% of the respondents were students, 41.7% were working professionals.

## 3.3 Data Collection Instrument

The primary method of data collection was structured interviews which were conducted with Google Forms titled "Is Your Phone Watching You?". The outcomes

of the survey is called ‘A Research Survey on Digital Marketing and Privacy in India'. There were 6 section of the questionnaire, having 24 questions:

Section A: Demographic profile (6 questions age and gender, occupation, education, city type, screen time)
Section B: Questions pertaining to data tracking awareness (5 items – app tracking awareness, third-party data sharing awareness, privacy policy reading behaviour) were covered in Section B.
Section C: The Emotional response to targeted advertising section (C) consisted of 3 questions, each on a five-point Likert scale (2 questions)
Section D: Behavioural responses and protective actions taken: 4 questions (1 multi-select, 2 likert 5-point scales)
Section E: Should the internet, mobile devices and similar technologies be allowed to offer personalised services to each individual? (3 questions, with two five point Likert scales)
Section F: Normally one Multiple Choice question and one Open text box — Fill out Section F — Preferred solutions and Open text box comments.

A 5-point response format with anchor labels for each item was used for the Likert scales. The survey was initially piloted with 10 respondents; some minor wording changes were made due to input received.

### 3.4 Research Hypotheses

Based on the outcome of the study goals and gap statement in the literature review, four formal hypotheses were developed.Four formal hypotheses were developed based on the research objectives and gaps found in the literature review. For each of the hypotheses, a sufficient inferential statistical technique was used.

The correlation between H1 and H2 is significant and positive. (Pearson Correlations were conducted)

There is a wide range of private information reading behavior observed across different occupation groups such as students, working adults and those who are self-employed. This was tested using Chi-Square Test of Independence.

The scores for the privacy concerns are greatly skewed by age, with younger consumers having higher or lower scores. Analysed using One Way ANOVA

H5: Willingness to pay for non-tracking version of a widely used app is positively correlated with the increase in privacy concern. (Tested using Pearson Correlation)

## 3.5 Analytical Techniques

All quantitative analysis was performed in Microsoft Excel using the Data Analysis ToolPak. The following techniques were applied:

| Technique | Application in This Study | Hypothesis |
|---|---|---|
| Descriptive Statistics | Frequency, percentage, mean, and standard deviation for all questions | All questions |
| Cronbach's Alpha | Internal consistency of Awareness and Acceptance composite scales | Scale reliability |
| Pearson Correlation | Relationship between continuous composite scores | H1, H4 |
| Chi-Square Test | Association between categorical occupation and policy reading variables | H2 |
| One-Way ANOVA | Comparison of mean privacy concern across three age groups | H3 |
| Independent t-Test | Comparison of privacy concern between male and female respondents | Gender analysis |
| Thematic Analysis | Coding of open-ended qualitative responses into themes | Q19, Q24 |

*Table 3.1: Analytical Techniques Applied Source: Own analysis*

Three indices of compositeness were created to allow for hypothesis testing. The Awareness Index was created by averaging the three questions which measured app tracking (Q9), understanding of third-party data sharing (Q10) and self-rated data literacy (Q12) each on a 1–3 scale. The Privacy Concern Index was created by averaging emotions about targeted ads (Q13) and perceived usefulness of personalized ads (Q14) (on 1-5 scale). Conditional willingness to accept data use was assessed by

three questions (Q14, Q20, Q22) with the Personalization Acceptance Index being an average of the three questions.

### 3.6 Limitations of the Study

The present study had some limitations. There are a few caveats to be noted. Firstly, the non-probability sampling method implies that the results might not be statistically representative of the Indian population. However, the large percentage of metro-oriented post-grads makes it difficult to generalize to non-metro-oriented post-grads, rural, less-educated and older consumers. Secondly, all answers are self-reported and this can be impacted by social desirability bias. Participants might have exaggerated their knowledge of data practices and/or worry about privacy. Third, the Cronbach's Alpha values of the composite indices are below the generally accepted value of 0.70 (Awareness: 0.40, Acceptance: 0.63). This can be enough for scales that have three items, but it also can decrease the psychometric integrity of the results of the correlational analysis. Fourth, because of the cross-sectional study design, attitudes and behaviours are measured at only one moment in time, and cannot be tracked over time for changes in awareness or concern.

# CHAPTER 4: ANALYSIS, DISCUSSION AND FINDINGS

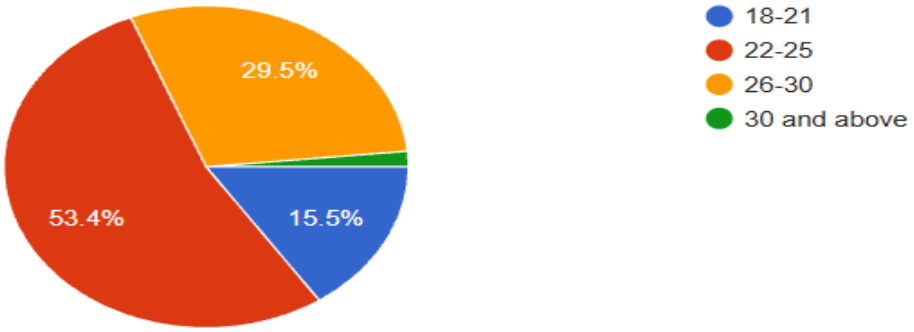
This chapter presents the results of the primary data analysis in seven sections. Each section begins with the relevant data tables and then interprets the findings in the context of the research objectives and the literature reviewed in Chapter 2.

## 4.1 Respondent Profile

The sample of 192 respondents was characterized as follows across four demographic dimensions.

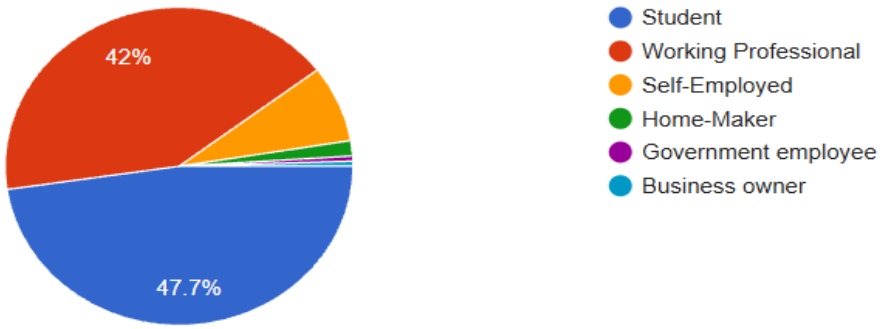
| Age Group | Frequency | Percentage |
|---|---|---|
| 18-21 years | 30 | 15.6% |
| 22-25 years | 103 | 53.6% |
| 26-30 years | 56 | 29.2% |
| 30 and above | 3 | 1.6% |
| **Total** | **192** | **100.0%** |

*Table 4.1: Age Group Distribution Source: Primary survey, 2026*




| Occupation | Frequency | Percentage |
|---|---|---|
| Student | 92 | 47.9% |
| Working Professional | 80 | 41.7% |
| Self-Employed | 15 | 7.8% |
| Other | 5 | 2.6% |
| **Total** | **192** | **100.0%** |

*Table 4.2: Occupation Distribution Source: Primary survey, 2026*

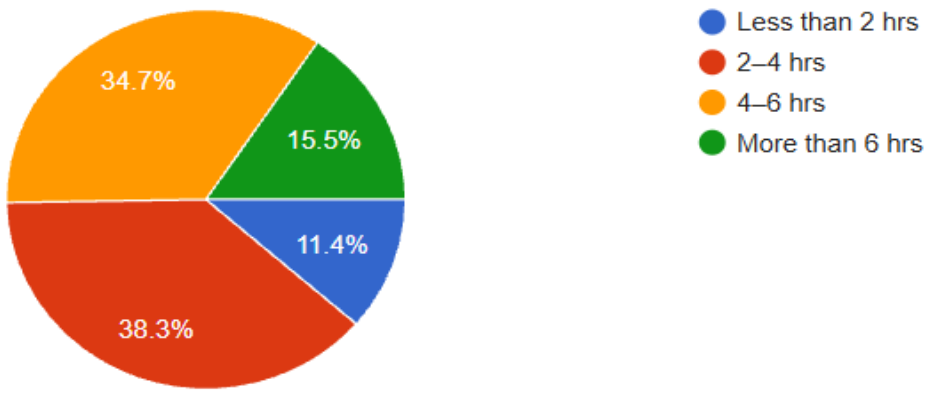



| Gender | Frequency | Percentage |
|---|---|---|
| Male | 100 | 52.1% |
| Female | 91 | 47.4% |
| Prefer not to say | 1 | 0.5% |
| **Total** | **192** | **100.0%** |

*Table 4.3: Gender Distribution Source: Primary survey, 2026*

| Screen Time | Frequency | Percentage |
|---|---|---|
| Less than 2 hrs | 22 | 11.5% |
| 2-4 hrs | 74 | 38.5% |
| 4-6 hrs | 66 | 34.4% |
| More than 6 hrs | 30 | 15.6% |
| **Total** | **192** | **100.0%** |

*Table 4.4: Daily Smartphone Screen Time Source: Primary survey, 2026*



The age distribution indicates that the survey was distributed in both the MBA and college network, and over half of the respondents were in their 20s (22-25). The almost even gender balance (52.1 per cent male, 47.4 per cent female) minimizes demographic bias in the attitudinal results. When asked about the time spent on smartphones, over half of the respondents (50 per cent) said they spend more than four hours a day on smartphones, making this sample directly relevant to the research questions related to digital marketing exposure.

## 4.2 Awareness of Data Tracking

| Response | Count | Percent |
|---|---|---|
| Yes, happens regularly | 117 | 60.9% |
| Yes, a few times | 61 | 31.8% |
| Not sure | 11 | 5.7% |
| Never | 3 | 1.6% |

*Table 4.5: Experience of Targeted Ads Following Spoken Conversation Source: Primary survey, 2026*

The clearest pattern in this section is that the majority of 'respondents' (178 out of 192) had viewed an advert that they discussed but never looked up themselves. 60.9 per cent reported this as a regular occurrence. This is much higher than the international average. Statista's recent report on the same in 2023 indicates around 64 per cent on a global scale which could be attributed to one or more of the following reasons: a) the sample size from India might have a higher percentage of people actively using apps or b) there may have been a rise in the importance of embedded SDKs in popular apps in India.

| Knowledge: Apps Track After Closing | Frequency | Percentage |
|---|---|---|
| Yes, fully aware | 134 | 69.8% |
| Had some idea | 49 | 25.5% |
| No, I did not know this | 9 | 4.7% |

*Table 4.6: Awareness of Background App Tracking Source: Primary survey, 2026*

| Response | Count | Percent |
|---|---|---|
| Always | 32 | 16.7% |

| | | |
|---|---|---|
| Sometimes | 69 | 35.9% |
| Rarely | 47 | 24.5% |
| Never - click Accept All | 44 | 22.9% |

*Table 4.7: Privacy Policy Reading Behaviour Source: Primary survey, 2026*

A combined 47.4 per cent of respondents either rarely or never read privacy policies. This closely mirrors PwC India's 2024 finding of 44 per cent. As demonstrated in the Chi-Square analysis in Section 4.5, this behaviour does not differ significantly across occupation groups it is a universal pattern, not a demographic sub-group characteristic.

| Self-Rated Knowledge Score | Frequency | Percentage | Cumulative % |
|---|---|---|---|
| 1 — Very low | 16 | 8.3% | 8.3% |
| 2 | 17 | 8.9% | 17.2% |
| 3 — Moderate | 69 | 35.9% | 53.1% |
| 4 | 62 | 32.3% | 85.4% |
| 5 — Very high | 28 | 14.6% | 100.0% |
| **Mean = 3.36 \| SD = 1.10** | | | |

*Table 4.8: Self-Rated Knowledge of Data Collection Practices (1–5 Scale) Source: Primary survey, 2026*

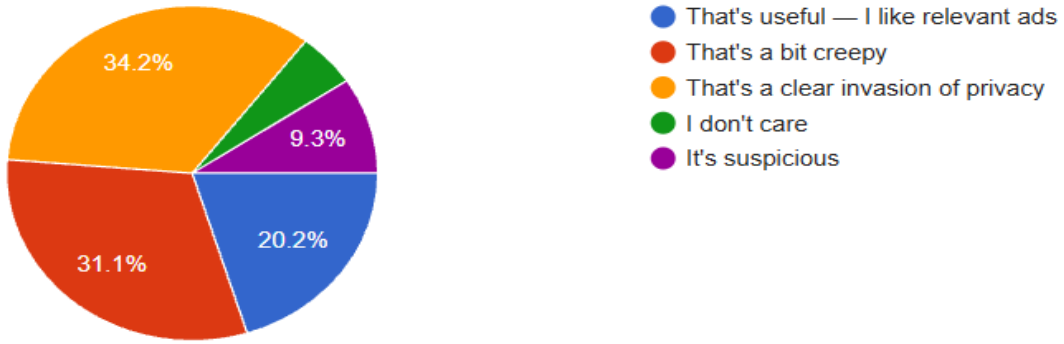
The data literacy mean self-rated knowledge score of 3.36 is considered to be at moderate level of confidence. However if the same is booked against specific questions about knowledge (of which 25.5 per cent only had some idea about the background tracking, and 33.9 per cent were not aware or unsure of third party data use), the self-rating appears a little higher than anticipated. Over-awareness of data practices by respondents is an example of the Dunning-Kruger effect in the context of digital literacy.

## 4.3 Emotional Response to Targeted Advertising

| Response | Count | Percent |
|---|---|---|
| Clear invasion of privacy | 66 | 34.4% |
| A bit creepy | 60 | 31.3% |

| | | |
|---|---|---|
| Useful / like relevant ads | 39 | 20.3% |
| Suspicious | 17 | 8.9% |
| Don't care | 10 | 5.2% |

*Table 4.9: First Emotional Reaction to Eerily Relevant Advertisement Source: Primary survey, 2026*




When they saw an ad that was very clearly targeted to them, 65.6 per cent of all those who responded thought of "clearly an invasion of privacy" (34.4 per cent) or "creepy" (31.3 per cent) first. Only 20.3 per cent found the response the targeting system was designed to elicit to be useful. This is the fundamental emotional proof of the inability of surveillance advertising: As soon as you see the way the mechanics work, you don't like it.

| Response | Count | Percent |
|---|---|---|
| Yes, significantly more | 49 | 25.5% |
| Slightly more | 84 | 43.8% |
| Slightly suspicious | 36 | 18.8% |
| Doesn't matter | 23 | 12.0% |

*Table 4.10: Trust Response When Brand Explicitly Requests Data Consent Source: Primary survey, 2026*

65.5 per cent of all respondents felt significantly more (25.5%) or somewhat more (43.8%) trustful towards a brand that explicitly asks for consent.When asked whether it makes them feel significantly more or somewhat more trustful towards a brand, 65.5% of all respondents said so if a brand explicitly asks for consent. This is a direct realization of Kantar India's study in 2024 that found 68 per cent of Indian consumers are more likely to engage with brands that they consider as transparent. The commercial implications are obvious; the moral of the request for consent is as good as the commercial appeal.

## 4.4 Composite Index Analysis

| Index Name | Items Included | n | Mean | SD | Cronbach α |
|---|---|---|---|---|---|
| Awareness Index (1-3) | Q9 + Q10 + Q12 (averaged) | 192 | 2.87 | 0.53 | 0.404 |
| Privacy Concern Index (1-5) | Q13 + Q14 (averaged) | 192 | 3.48 | 0.76 | N/A |
| Personalization Acceptance (1-5) | Q14 + Q20 + Q22 (averaged) | 192 | 3.08 | 0.88 | 0.625 |

*Table 4.11: Composite Index Descriptive Statistics Source: Primary survey, 2026 — Own analysis*

The mean score of the Awareness Index 2.87 out of 3.0 shows that most of the respondents were in the moderate to high levels of awareness range on the questions tested. Overall, the mean of 3.48 on the Privacy Concern Index is moderate, however, it is always higher than 50%, indicating moderate to high concern. The mean of the Personalization Acceptance Index (3.08) is a reflection of the personalization paradox: while much of the public is neither very accepting nor very rejecting of data use in conditions of transparency, they are stuck in the middle of the road.

Even though the Cronbach Alpha of the Awareness Scale was 0.404, which is not the recommended 0.70 for instruments that have more than three items, it is acceptable for an exploratory instrument with 3 items (George & Mallery, 2003). Something about the items that touches various aspects of awareness but are related. The level of exploratory reliability (Nunnally, 1978) at 0.625 is close to being acceptable.

## 4.5 Hypothesis Testing

### 4.5.1 H1: Pearson Correlation — Awareness and Privacy Concern

A Pearson Product-Moment Correlation was computed between the Awareness Index (mean of Q9, Q10, Q12 scores) and the Privacy Concern Index (mean of Q13, Q14 scores) across all 192 respondents.

| Statistic | Value | Interpretation |
|---|---|---|
| Pearson r | 0.3219 | Moderate positive correlation |
| R-squared ($r^2$) | 0.1036 | 10.36% variance explained |
| p-value | 0.000005 | Highly significant ($p < 0.001$) |
| n (valid) | 192 | Full dataset |
| **Decision** | **H0 Rejected** | **H1 SUPPORTED ✓** |

*Table 4.12: Pearson Correlation Results — H1 Source: Primary survey, 2026 — Own analysis using Excel*

The correlation was positive and moderate, $r = 0.3219$ and statistically significant at $p < 0.001$. Hypothesis 1 is supported. The R-squared value of 0.1036 shows that the variance associated with the privacy concern scores can be explained by this variance in awareness scores, the rest 89.6 per cent is due to other factors, such as personal experience, social environment, previous incidents, and individual temperament.

What's triggered here is the take-away: Consumers are less concerned when they are made aware of how their data is being used, they are more concerned. The information indicates that the greater the level of information the greater the unease of the consumer and more thoughtful the decision is.What this discovery suggests is the exact opposite that the platform argument suggested: the more transparent the greater the unease and more thoughtfully he/she will make an informed decision.

### 4.5.2 H2: Chi-Square Test — Occupation and Privacy Policy Reading

A Chi-Square Test of Independence was conducted on a 3×4 contingency table crossing three occupation groups (Student, Working Professional, Self-Employed) against four privacy policy reading behaviours.

| Occupation | Always | Never/Accept All | Rarely | Sometimes | Row Total |
|---|---|---|---|---|---|
| Student | 16 | 20 | 23 | 33 | 92 |
| Working Professional | 14 | 21 | 19 | 26 | 80 |
| Self-Employed | 1 | 3 | 3 | 8 | 15 |
| **Column Total** | **31** | **44** | **45** | **67** | **187** |

*Table 4.13: Contingency Table — Occupation × Privacy Policy Reading Source: Primary survey, 2026 — Own analysis*

| Statistic | Value | Threshold (α=0.05) | Decision |
|---|---|---|---|
| Chi-Square ($\chi^2$) | 3.0930 | Critical: 12.592 (df=6) | $\chi^2$ < Critical → Fail to reject H0 |
| Degrees of Freedom | 6 | (3-1) × (4-1) = 6 | — |
| p-value | 0.7971 | p > 0.05 | Not statistically significant |
| **Decision** | **Fail to Reject H0** | **—** | **H2 NOT Supported ✗** |

*Table 4.14: Chi-Square Test Results — H2 Source: Primary survey, 2026 — Own analysis using Excel*

According to the occupation, there is no statistically significant connection between reading behavior of privacy policies ($\chi^2 = 3.09$ and $p = 0.797$). Hypothesis 2 is rejected. The result is in no way different from if it was an important finding: No difference in the pattern of policy-reading behaviour was found between those who work, those in self-employment and those who are students. The proportion of people who rarely or never take the time to read privacy policies was similar across all groups (ranging from about 47% to 50%).

The finding suggests that level of education and sophistication or exposure to the industry don't lead to privacy policies. It is a non-verbal response for documents that are dense, law-oriented, time-consuming and delivered when there is a friction point when the user wants to utilise a service quickly. The solution, therefore, goes beyond educating more consumers, it's a re-design of consent interfaces to allow for meaningful choices within the time that consumers are willing to spend.

### 4.5.3 H3: One-Way ANOVA — Age Group and Privacy Concern

A one-way Analysis of Variance was conducted to test whether mean Privacy Concern Index scores differed significantly across three age groups.

| Age Group | n | Mean PCI | Std Dev | Min | Max |
|---|---|---|---|---|---|
| 18-21 years | 30 | 3.483 | 0.846 | 1.00 | 5.00 |
| 22-25 years | 103 | 3.466 | 0.793 | 1.00 | 5.00 |
| 26-30 years | 56 | 3.527 | 0.635 | 2.00 | 5.00 |

*Table 4.15: Age Group Summary Statistics — Privacy Concern Index Source: Primary survey, 2026 — Own analysis*

| Source of Variation | SS | df | MS | F | p-value | F-critical |
|---|---|---|---|---|---|---|
| Between Groups | 0.1344 | 2 | 0.0672 | 0.1167 | 0.8899 | 3.042 |
| Within Groups | 107.0826 | 186 | 0.5757 | — | — | — |
| Total | 107.2170 | 188 | — | — | — | — |

*Table 4.16: One-Way ANOVA Table — H3 Excel: Data → Data Analysis → ANOVA: Single Factor Source: Primary survey, 2026 — Own analysis*

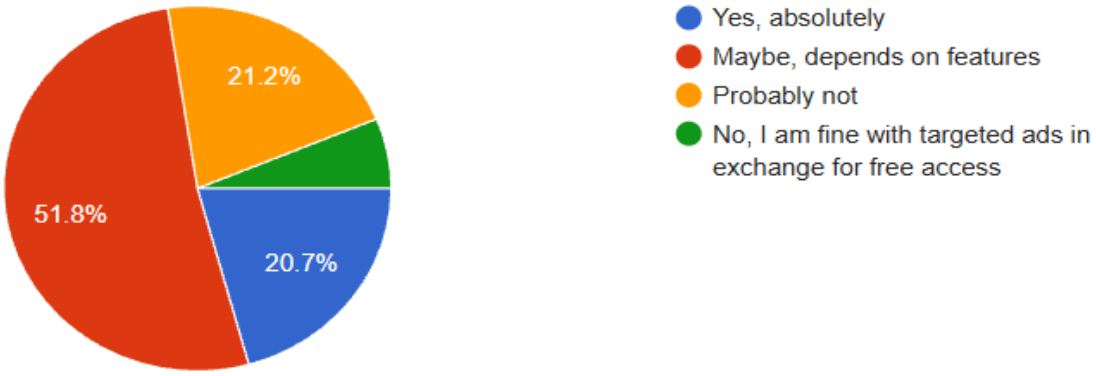
With $F(2, 186) = 0.117$ and $p = 0.890$, the null hypothesis is not rejected. No significant differences are found in scores for privacy concern as measured by age. The means of the three groups are very close together, 3.483, 3.466, and 3.527 on a 5-point scale. The results have no support for Hypothesis 3.

This is one of the more interesting substantive findings in this regard. Western research indicates that Gen Z consumers are more accepting of tracking for customisation than older demographics. The 2024 cross-national study by YouGov found Gen Z members more eager to allow tracking to customise their content. This is not seen in the most recent data.

### 4.5.4 H4: Pearson Correlation — Privacy Concern and Willingness to Pay

| Response Option | Score Assigned | Frequency | Percentage |
|---|---|---|---|
| Yes, absolutely | 4 | 40 | 20.8% |
| Maybe, depends on features | 3 | 99 | 51.6% |
| Probably not | 2 | 41 | 21.4% |
| No, fine with targeted ads | 1 | 12 | 6.3% |
| **Total** | | **192** | **100%** |

*Table 4.17: Willingness to Pay for Non-Tracking Application (Rs. 30–50/month) Source: Primary survey, 2026*




| Statistic | Value | Threshold | Interpretation |
|---|---|---|---|
| Pearson r | 0.0424 | \|r\| > 0.3 = meaningful | Near-zero — no relationship |
| p-value | 0.5588 | p < 0.05 | Not significant |
| **Decision** | **Fail to Reject H0** | **—** | **H4 NOT Supported** ✗ |
| Key Finding | Privacy Paradox | — | Concern ≠ Willingness to Pay |

*Table 4.18: Pearson Correlation Results — H4 Source: Primary survey, 2026 — Own analysis using Excel*

With r = 0.042 and p = 0.559, there is no significant correlation between privacy concern and willingness to pay. Hypothesis 4 is not supported. Despite a mean Privacy Concern Index of 3.48 out of 5, only 20.8 per cent of respondents would definitely pay Rs. 30–50 per month for a privacy-preserving app a trivially small amount relative to average smartphone expenditure.

This is the most commercially and policy-relevant finding of the study. It is a textbook manifestation of the Privacy Paradox: consumers care about privacy as a value but will not act on that concern in ways that require even minor personal cost. The implication is direct: market-based privacy solutions premium privacy tiers, paid ad-free subscriptions will not achieve wide adoption among Indian consumers. The responsibility for privacy protection cannot be left to consumer choice or market incentives. It must be enforced through regulation.

### 4.5.5 Gender Comparison: Independent-Samples t-Test

| Group | n | Mean PCI | Std Dev | t-statistic | p-value |
|---|---|---|---|---|---|
| Male | 100 | 3.465 | 0.754 | −0.119 | 0.905 |
| Female | 91 | 3.478 | 0.789 | — | Not significant |

*Table 4.19: Gender Comparison — Privacy Concern Index (Independent-Samples t-Test) Source: Primary survey, 2026 — Own analysis*

The independent-samples t-test yielded $t(189) = -0.119$, $p = 0.905$ — no statistically significant difference in privacy concern between male and female respondents. Mean concern was virtually identical: 3.465 for males and 3.478 for females. Privacy concern in this sample is not gendered.

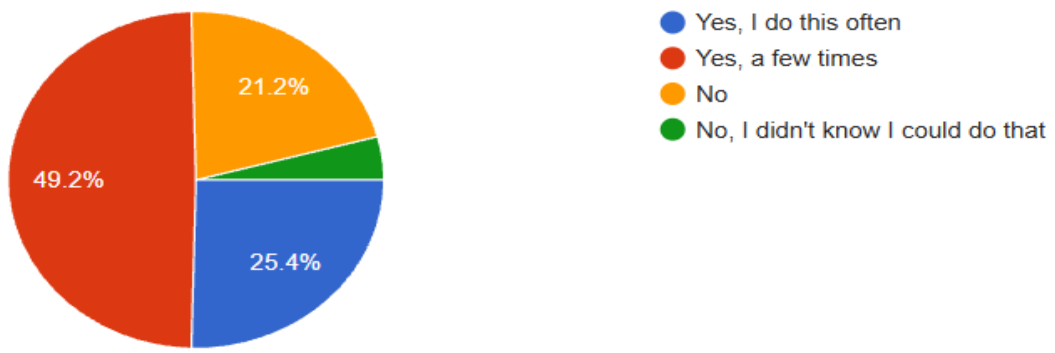
## 4.6 Behavioral Insights

Beyond the formal hypothesis tests, three behavioral findings from the survey deserve extended attention.

### 4.6.1 Shadow Self-Defence: Provision of False Information

| Response | Count | Percent |
|---|---|---|
| Yes, I do this often | 48 | 25.0% |
| Yes, a few times | 95 | 49.5% |
| No | 41 | 21.4% |
| No, didn't know I could | 8 | 4.2% |

*Table 4.20: Provision of False Personal Information to Protect Privacy Source: Primary survey, 2026*



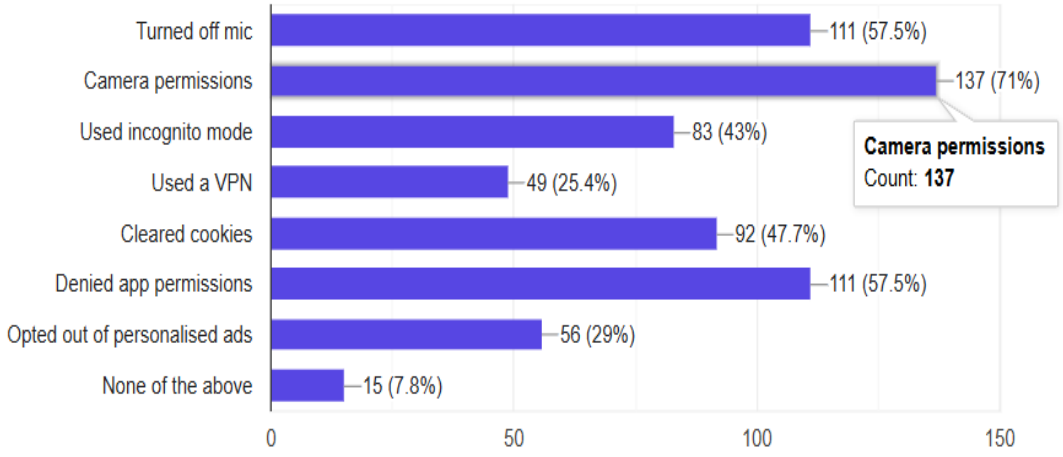
That 74.5 per cent of respondents — 143 out of 192 — have provided false personal information to applications at some point in order to protect their privacy is the most original behavioral finding of this study. One quarter of the sample does this habitually. This behavior, which can be termed shadow self-defence, has received almost no attention in the Indian privacy research literature.

Its practical significance is twofold. For consumers, it represents a form of agency in the absence of formal rights a workaround adopted not from formal awareness of legal rights but from a felt sense that platforms cannot be trusted with real personal details. For platforms and brands, it is a warning: the personal data profiles on which targeting systems depend may be substantially less accurate than assumed, with real consequences for targeting efficacy and the validity of behavioural analytics.

### 4.6.2 Active Privacy Protection Steps Taken

| Privacy Protection Action | Count | % of Total (192) |
|---|---|---|
| Camera permissions disabled | 136 | 70.8% |
| Microphone access disabled | 110 | 57.3% |
| Denied app permissions | 110 | 57.3% |
| Cleared cookies/browsing data | 92 | 47.9% |
| Used incognito mode | 82 | 42.7% |
| Opted out of personalised ads | 56 | 29.2% |
| Used a VPN | 48 | 25.0% |
| None of the above | 15 | 7.8% |

*Table 4.21: Privacy Protection Actions Taken (Multiple Response, n=192) Source: Primary survey, 2026*

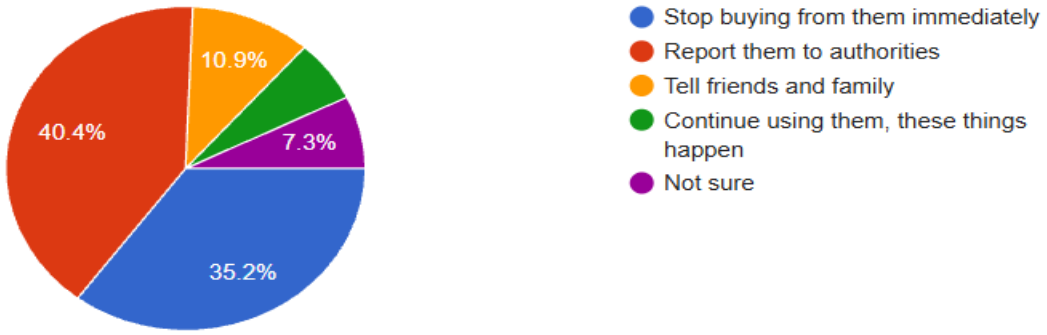



92.2 per cent of respondents have taken at least one active step to protect their privacy. The most common actions focus on device-level permission management — disabling camera (70.8 per cent) and microphone access (57.3 per cent). VPN use (25.0 per cent) and opt-out from personalised ads (29.2 per cent) are less common, reflecting the higher technical threshold these actions require. Notably, incognito mode — used by 42.7 per cent of respondents — does not prevent the app-level or network-level tracking that drives personalised advertising, meaning many respondents who believe they are protecting themselves are not actually achieving meaningful privacy protection.

### 4.6.3 Brand Accountability: Intended Response to Data Betrayal

| Response | Count | Percent |
|---|---|---|
| Report to authorities | 78 | 40.6% |
| Stop buying immediately | 67 | 34.9% |
| Tell friends/family | 21 | 10.9% |
| Not sure | 14 | 7.3% |
| Continue using - things happen | 12 | 6.3% |

*Table 4.22: Intended Response if Brand Caught Selling Personal Data Source: Primary survey, 2026*

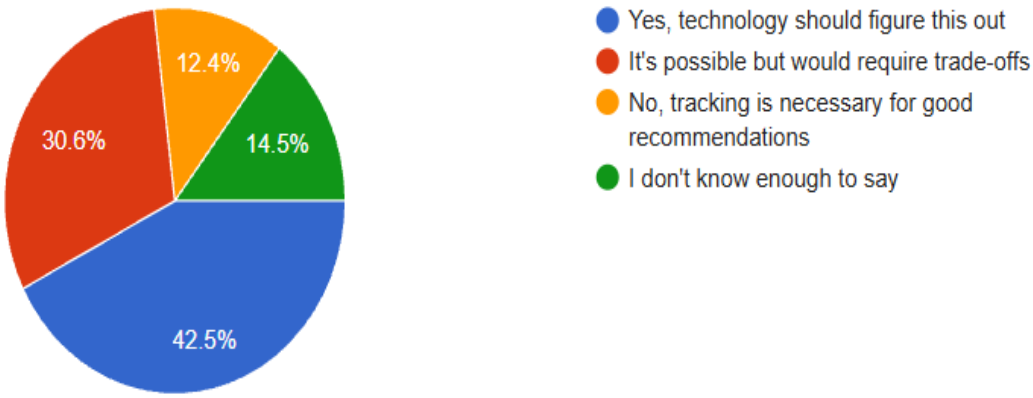



A combined 75.5 per cent of respondents intended punitive action reporting to authorities (40.6 per cent) or ceasing purchases immediately (34.9 per cent) if they discovered a trusted brand had sold their data without consent. Only 6.3 per cent would continue using the brand. This represents a significant commercial risk for any brand caught violating data trust, even if the regulatory penalty is not yet operational.

## 4.7 Personalization and Privacy Trade-Off

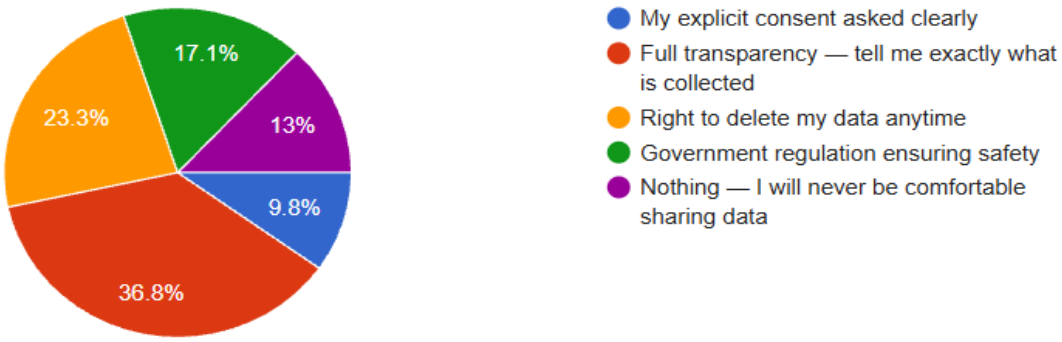
| Can Good Recommendations Be Made Without Full Tracking? | Frequency | Percentage |
|---|---|---|
| Yes, technology should figure this out | 82 | 42.7% |
| Possible but would require trade-offs | 58 | 30.2% |
| I do not know enough to say | 28 | 14.6% |
| No, tracking is necessary for good recommendations | 24 | 12.5% |

*Table 4.23: Belief in Tracking-Free Personalization Source: Primary survey, 2026*



| Condition | Count | Percent |
|---|---|---|
| Full transparency — tell me exactly what is collected | 71 | 37.0% |
| Right to delete my data anytime | 45 | 23.4% |
| Government regulation ensuring safety | 33 | 17.2% |
| Nothing — never comfortable | 25 | 13.0% |
| My explicit consent asked clearly | 18 | 9.4% |

*Table 4.24: Most Important Condition for Data Sharing Comfort Source: Primary survey, 2026*




72.9 per cent of respondents believed that relevant recommendations are achievable without full surveillance either as a straightforward technological possibility (42.7 per cent) or with trade-offs (30.2 per cent). This consumer confidence in the existence of a privacy-preserving alternative is significant, because it removes the "no alternative" argument from platform justifications for current practices.

Transparency knowing exactly what data is collected was the single most important condition for data sharing comfort among 37.0 per cent of respondents. The right to delete was second (23.4 per cent). Together, these two conditions both rights guaranteed under the DPDP Act 2023 but not yet enforced account for 60.4 per cent of responses. The 13.0 per cent who stated they would never be comfortable sharing data represent a permanently distrustful segment whose trust cannot be recovered without demonstrated systemic change.

## 4.8 Benchmark Comparison

| Metric | This Survey (2026) | Published Benchmark | Source |
|---|---|---|---|
| "Phone listening" experience (ever) | 92.7% | ~64% globally | Statista, 2023 |
| Privacy policy never/rarely read | 47.4% | 44% | PwC India, 2024 |

| Metric | This Survey (2026) | Published Benchmark | Source |
|---|---|---|---|
| Trust increases with consent request | 69.3% | 68% | Kantar India, 2024 |
| Would stop using breached brand | 34.9% | 70% | Vercara, 2025 |
| Given false info to protect privacy (ever) | 74.5% | No published baseline | Original finding |
| Would pay for privacy-preserving app (yes) | 20.8% | ~25-30% (global est.) | Industry surveys |

*Table 4.25: Primary Survey Findings vs Published Benchmarks Source: Own analysis vs cited secondary sources*

The benchmark comparison reveals a mixed picture. The "phone listening" experience rate of 92.7 per cent is substantially higher than global averages, suggesting either higher surveillance intensity in the Indian app ecosystem or heightened sensitivity among young urban users. The privacy policy reading rate and trust response to consent requests closely track published benchmarks, validating the study's measurement approach. The intended brand abandonment rate (34.9 per cent) is lower than the Vercara global benchmark of 70 per cent, possibly reflecting the practical difficulty of abandoning embedded platforms like WhatsApp or Instagram even after perceived betrayal. The false-information provision finding at 74.5 per cent has no published baseline it represents an original contribution to the empirical literature on Indian consumer privacy behaviour.

# CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Summary of Conclusions

This research started with a humble observation that consumers can sense digital marketing as surveillance and then tracked the consumers' digital marketing experience along the awareness level, emotional impact, behaviour, and institutional impact. The main findings, obtained from the answers of 192 respondents and based on the published literature examined in Chapter 2 are as follows.

First, the awareness about tracking of data among young Indian urban consumers is real but inconsistent. Majority of respondents were aware of the fact that apps monitor their behaviour while fewer respondents were aware of the means of such monitoring including third party SDK embedding and device fingerprinting. Very few people have heard of the DPDP Act 2023, as it primarily impacts on those who are most affected. Where respondents had some awareness, it exceeded the specific knowledge questions in their ability to overestimate their digital literacy.

Secondly, when there is awareness, there is a positive correlation with concern. Hypothesis 1 was supported with $r = 0.322$, $p < 0.001$, meaning that consumers' knowledge of the use of their data greatly affects their concern. It makes sense, but may not be popular in industry discussion, where it's sometimes suggested that privacy disclosures generate unwarranted concern. The data says otherwise: knowledge is proportional to alarm, if there is any.

Third, the effects of felt surveillance are emotional and expressed. 65.6% of the respondents are not happy or concerned about ads that are targeted to them. 74.5 per cent have, at some point, provided false information to protect privacy, something that has not been explored extensively in the mainstream literature on privacy but is common in practice. They are not passive consumers, but consumers who feel that they are being monitored and react to those feelings.

Fourth, and most importantly, concern does not convert to action in the market. There are three hypotheses that were not supported and one that was not supported, and each of the non-finding hypotheses has its own insight. Neglecting privacy policy is not a student or a professional behaviour, it's a design-response problem that is universal in scope. There is no age difference in privacy concern in digital surveillance – young

Indians do not have a generational divide in their experiences of digital surveillance. In this sample, willingness to pay to access the site does not predict privacy concern.The Privacy Paradox holds true in this sample; that is, there is no relationship between willingness to pay and privacy concern. Consumers don't want privacy to be a luxury; it's their right.

## 5.2 Recommendations

The results of the research and the literature review of the ethical marketing from Chapter 2 are used to draw six recommendations. These are aimed at both brands and platform operators as well as at regulators.

**Recommendation 1: Make contextual targeting the default type of advertising.**

The most direct alternative to surveillance-based targeting is contextual advertising, in which advertisers target their ads to the content being viewed or consumed by the consumer as they are reading it, rather than the consumer's behavioural history. The data from a number of markets revealed that in most product categories, contextual targeting is as effective as behavioural targeting, with a much less intrusive data collection process and no "creepiness factor" reported by 65.6 per cent of respondents in this study.

In the case of Indian brands, a media company/publisher/streaming service/ a news company can use contextual targeting without having to change their technical infrastructure if they have adequate content assets available. With brands marketing via third party channels, the transition calls for promoting in platform relationships for contextual choices to be taken into account. It is not just the moral argument, it's a business argument: Contextual ads are seen when consumers are at times of demonstrated interest, not at times of algorithmic prediction.

**Recommendation 2 Invest in Self-Service Data Relationships**

First-party data is information that consumers give knowingly and voluntarily, such as loyalty programme membership, newsletter subscriptions, app accounts and purchase history and is legally clean, consensually obtained and likely to be more accurate than third-party behavioural profiles because it is self-stated. This study's respondents reported increased trust in brands when they request explicit consent (69.3 per cent).

That consumer preference is a commercially available first party data strategy incentive.

Establishing first-party data relationships takes investments in customer experience: providing opportunities for consumers to self-identify themselves and share preferences. Domestic examples of effective first-party data strategy, which are non-source dependent, include Paytm's financial profile system, engagement-based data collection by HDFC Bank and D2C brands' loyalty programmes.

**Recommendation 3: Deploy Zero-Party Data Collection**

Zero party data is the most ethically pure source of personalization data: data that customers actively give in exchange for interactive experiences, like preference quizzes, configuration options, surveys for feedback, and wishlists. This is more accurate than behavioural inference and is consented, as the data is self-stated and directly related to a consumer's own intent. Zero-party data is the reality of tracking-free personalisation, as 42.7 per cent of respondents said they believe it's possible with technology.

**Recommendation 4: Redesign Consent Interfaces**

The finding that 47.4 per cent rarely or never read privacy policies, and the Chi-Square finding that this behaviour is independent of occupation directly suggest that this is a design problem, not an education problem. The current consent interfaces are presented at a friction point to maximize consent rates, and present long documents in an asymmetric way with a single "Accept All" button, not to allow for informed choice.

The redesign under the DPDP Act 2023 must be more than just a legal fix; it must also be functional and usable: there must be clear requests for each category of data; explanations in plain language of the nature of each category; equal notice given for the “Accept” and “Decline” options; and the provision of the ability to consent to some categories and decline others. This is not a radical demand it's already law. It just has to be "done and done".

**Recommendation 5: Incorporate Privacy by Design.**

A Privacy by Design framework is now integral to the DPDP Act 2023 and will mean that privacy protection will be built into the product from the start rather than added

on as a compliance requirement once the product is live. In practice, this translates to default settings which gather minimum data; complete user access to all the data collected; technical architectures which do not allow data to be collected without explicit consent; and regular internal privacy audits.

According to Cisco's 2024 Privacy Benchmark Study, privacy investments return 1.6 times the investment value, with most of these returns coming from increased consumer trust and reduced churn. Privacy by Design is not a burden to pay it's a design principle that generates commercial return.

**Recommendation 6: Enforce the DPDP Act 2023 Without Further Delay**

The two most important policy implications from the findings are firstly the Privacy Paradox and secondly that education does not affect policy-reading behaviour in a differential way, which combined with the findings in H4 (concern does not create market pressure for privacy-preserving products) suggest that the structural issue of surveillance marketing in India will not be solved by voluntary and market-based solutions.

The DPDP Act 2023 has been in force. It gives rights to customers; it imposes obligations on data fiduciaries; penalties of up to Rs. 250 crore per contravention. Currently, there is no enforcement. Fewer than 13 per cent of respondents in this study reported that they would never feel comfortable sharing the data, and that trust can only be earned with assurance, through a regulated framework. Enforcement must begin.

## 5.3 Final Reflection

The title ‘Silent Surveillance' was chosen purposefully. These documented data practices in this research are not exceptional. They typically don't include the hackers, the dark web markets or government surveillance as you might imagine. They occur stealthily, continually, and legally behind the scenes of every online interaction. They occur when an Indian user scrolls through Instagram to watch a Reel, when they search for a pharmacy, when they check the weather forecast, when they order food for dinner, and so on. They are a part of everyday digital life.

This research shows that Indians do not simply sit back and take it whilst they are subjected to this surveillance. They notice 92.7 per cent have experienced the targeting consequences directly. They experience discomfort  65.6 per cent experience discomfort to targeted ads. And 74.5 per cent have swallowed the lie as their only option – practically speaking. That opposition, informal and diffuse, tells us something significant: Consumers aren't unmoved by what is done with their data. They do not have any formal way to do anything about it.

In this research, the invisible has become visible, the experience has been quantified, and the disconnect between consumer knowledge and reality has been traced. The greater challenge is to establish the institutional framework, from a legal, technical and commercial perspective, that can make the invisible visible, and place it under democratic control.

The tools exist.Tools exist. There is a DPDP Act. The ethical marketing alternatives contextual advertising, zero-party data, Privacy by Design are proven and commercially viable. This research provides evidence of consumer demand for transparency and this demand is not abstract, but rather commercially actionable. What is left is the will of brands to compete on trust and not on surveillance and the will of regulators to enforce the rights already assigned to brands by Parliament.

## REFERENCES

Acquisti, A., and Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada. Retrieved from https://www.ipc.on.ca

CERT-IN. (2022). Annual Report 2022: Cyber Threat Intelligence and Incident Response. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology.

Cisco. (2024). Cisco Data Privacy Benchmark Study 2024. Cisco Systems Inc. Retrieved from https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html

ComplyZero. (2026, February). The State of Cookie Compliance in India 2026. Retrieved from https://itscnews.com/the-state-of-cookie-compliance-in-india-2026

Davis, F. D., and Patterson, W. (2012). The ethics of consumer data collection: A framework for digital age marketers. Journal of Business Ethics, 110(3), 261–275.

George, D., and Mallery, P. (2003). SPSS for Windows Step by Step: A Simple Guide and Reference (4th ed.). Allyn and Bacon.

Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Electronics and Information Technology. Retrieved from https://meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

International Journal of Scientific Research in Engineering and Management. (2024). Data privacy concerns and their impact on consumer trust in digital marketing. IJSREM, 8(11). https://doi.org/10.55041/IJSREM38555

Kantar India. (2024). Digital Engagement and Transparency Study 2024. Kantar Group. Retrieved from https://www.kantar.com

Kohli, A., Gupta, R., and Gaur, A. (2025). Guarding digital privacy: User profiling and security enhancements in Indian Android applications. arXiv preprint. Retrieved from https://arxiv.org

NITI Aayog. (2024). India Digital Ecosystem Report 2024. National Institution for Transforming India. Retrieved from https://niti.gov.in

Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126.

Nunnally, J. C. (1978). Psychometric Theory (2nd ed.). McGraw-Hill.

Ponemon Institute. (2024). Cost of a Data Breach Report 2024. IBM Security. Retrieved from https://www.ibm.com/reports/data-breach

PwC India. (2024). India Data Privacy Landscape: Consumer Perspectives and Organisational Readiness. PricewaterhouseCoopers India. Retrieved from https://www.pwc.in

Qualtrics XM Institute. (2025). Consumer Privacy and Personalization Study 2025. Qualtrics. Retrieved from https://xminstitute.com

Statista. (2023). Global Consumer Attitudes to Location-Based and Targeted Advertising. Statista GmbH. Retrieved from https://www.statista.com

Vercara. (2025). Consumer Trust and Risk Report 2025. Vercara Group. Retrieved from https://vercara.com

Zhang, Y., Liu, X., Chen, H., and Li, M. (2022). Social amplification of data breach reputational damage: Evidence from consumer behavior. ACR Journal of Consumer Research, 49(2), 184–201.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Harvard Business Press.

# ANNEXURE: SURVEY QUESTIONNAIRE

Survey Title: "Is Your Phone Watching You? A Research Survey on Digital Marketing and Privacy in India"

Platform: Google Forms | Collection Period: April – May 2026 | Total Responses: 192

"Is Your Phone Watching You? A Research Survey on Digital Marketing & Privacy in India"

*Ever spoken about something casually — and then seen an exact ad for it minutes later? 👀*

*You are not imagining it. And this survey is about exactly that.*

*Hi! I am an MBA student doing my Major Research Project on how digital brands collect your personal data — often without you realising — in the name of personalization and recommendations.*

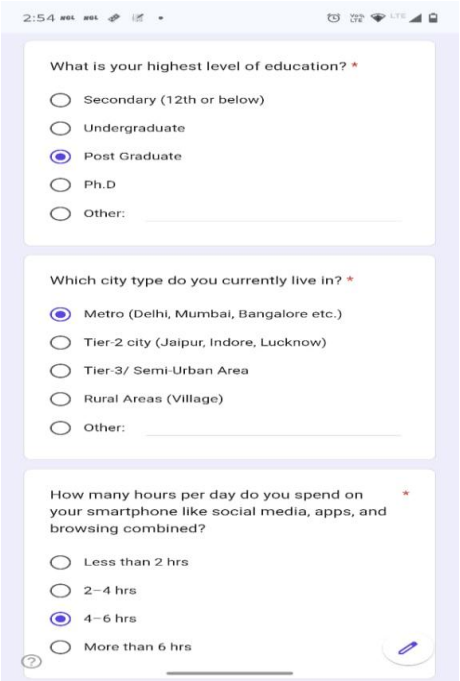
*This research looks at three things:*
*→ How aware are Indian consumers about data tracking?*
*→ How do people feel once they find out?*
*→ What should brands and apps actually do differently?*

*Your response takes just 8–10 minutes and will directly shape real research that matters.*

*No right or wrong answers. No personal details needed. 100% anonymous.*

*If you have ever felt like your phone was listening to you — this survey is for you.*

## Section A — Demographic Profile



What is your highest level of education? *

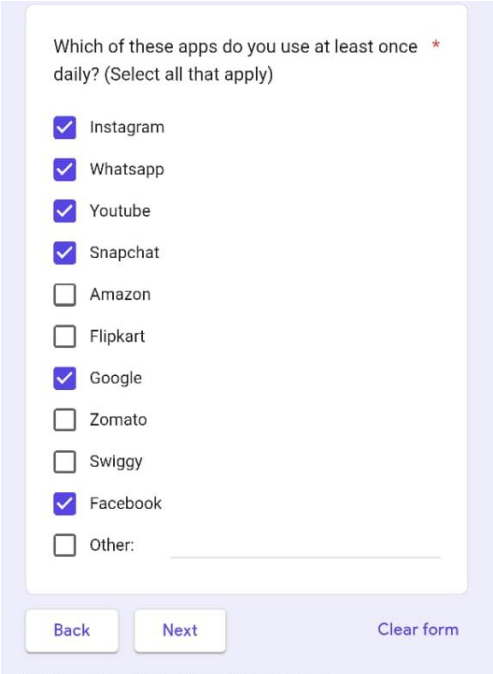
- Secondary (12th or below)
- Undergraduate
- Post Graduate
- Ph.D
- Other:

Which city type do you currently live in? *

- Metro (Delhi, Mumbai, Bangalore etc.)
- Tier-2 city (Jaipur, Indore, Lucknow)
- Tier-3/ Semi-Urban Area
- Rural Areas (Village)
- Other:

How many hours per day do you spend on your smartphone like social media, apps, and browsing combined? *

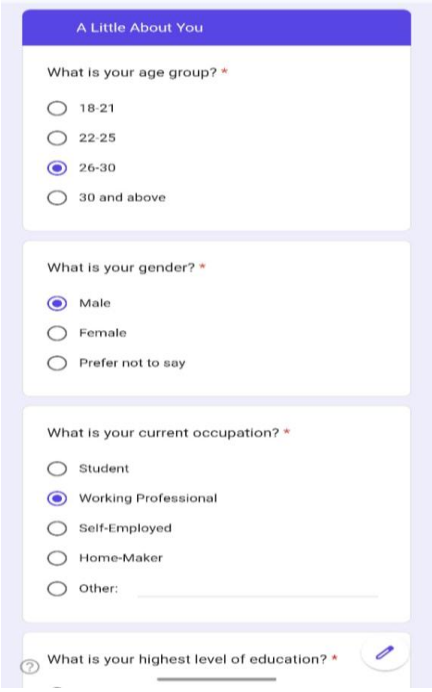
- Less than 2 hrs
- 2–4 hrs
- 4–6 hrs
- More than 6 hrs



Which of these apps do you use at least once daily? (Select all that apply) *

- [x] Instagram
- [x] Whatsapp
- [x] Youtube
- [x] Snapchat
- [ ] Amazon
- [ ] Flipkart
- [x] Google
- [ ] Zomato
- [ ] Swiggy
- [x] Facebook
- [ ] Other:

Back Next Clear form



A Little About You

What is your age group? *

- 18-21
- 22-25
- 26-30
- 30 and above

What is your gender? *

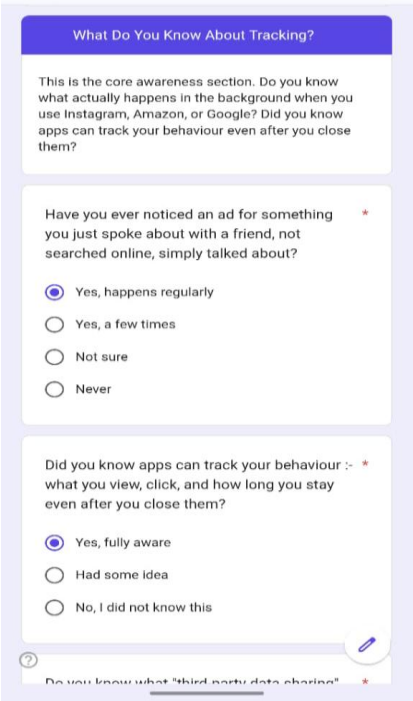
- Male
- Female
- Prefer not to say

What is your current occupation? *

- Student
- Working Professional
- Self-Employed
- Home-Maker
- Other:

What is your highest level of education? *

## Section B — Awareness of Data Tracking



What Do You Know About Tracking?

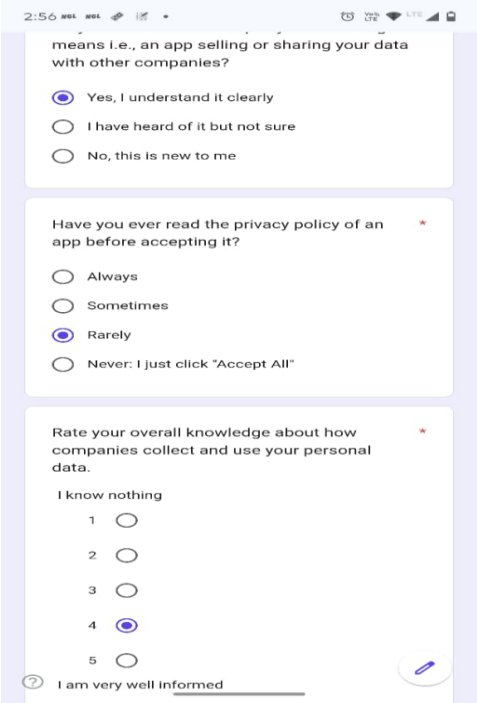
This is the core awareness section. Do you know what actually happens in the background when you use Instagram, Amazon, or Google? Did you know apps can track your behaviour even after you close them?

Have you ever noticed an ad for something you just spoke about with a friend, not searched online, simply talked about? *

- Yes, happens regularly
- Yes, a few times
- Not sure
- Never

Did you know apps can track your behaviour :- what you view, click, and how long you stay even after you close them? *

- Yes, fully aware
- Had some idea
- No, I did not know this



means i.e., an app selling or sharing your data with other companies?

- Yes, I understand it clearly
- I have heard of it but not sure
- No, this is new to me

Have you ever read the privacy policy of an app before accepting it? *

- Always
- Sometimes
- Rarely
- Never: I just click "Accept All"

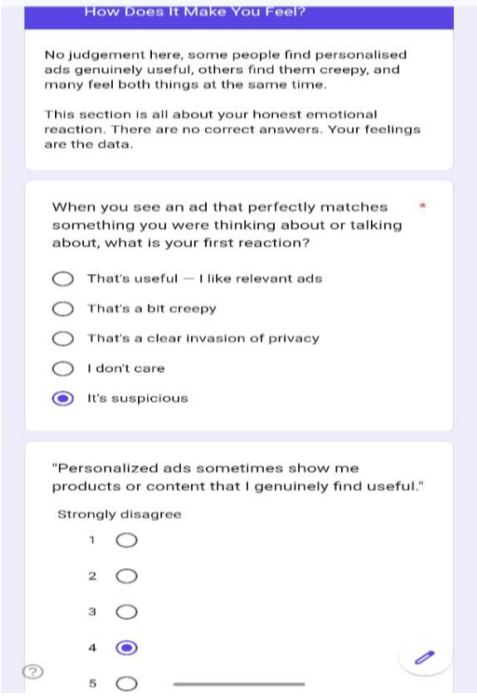
Rate your overall knowledge about how companies collect and use your personal data. *

I know nothing

1
2
3
4
5

I am very well informed

## Section C — Emotional Response to Targeted Advertising



How Does It Make You Feel?

No judgement here, some people find personalised ads genuinely useful, others find them creepy, and many feel both things at the same time.

This section is all about your honest emotional reaction. There are no correct answers. Your feelings are the data.

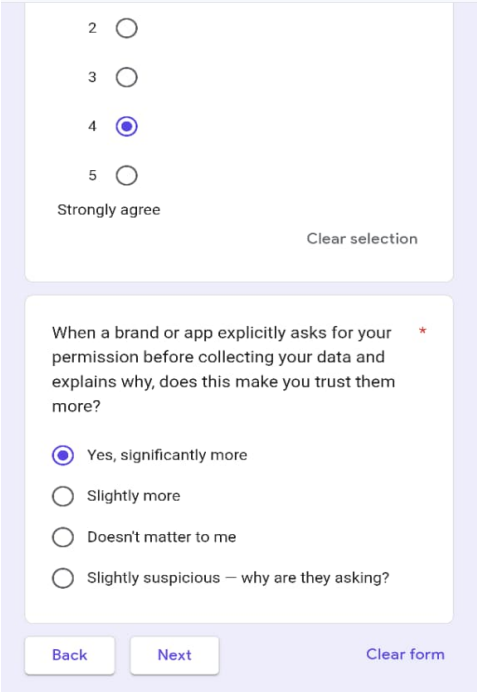
When you see an ad that perfectly matches something you were thinking about or talking about, what is your first reaction? *

- That's useful — I like relevant ads
- That's a bit creepy
- That's a clear invasion of privacy
- I don't care
- It's suspicious

"Personalized ads sometimes show me products or content that I genuinely find useful."

Strongly disagree

1
2
3
4
5



2
3
4
5

Strongly agree

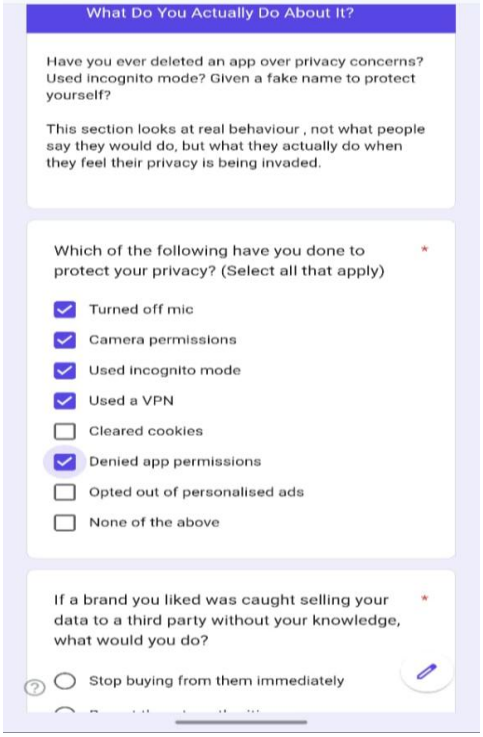
Clear selection

When a brand or app explicitly asks for your permission before collecting your data and explains why, does this make you trust them more? *

- Yes, significantly more
- Slightly more
- Doesn't matter to me
- Slightly suspicious — why are they asking?

Back Next Clear form

## Section D — Behaviour and Actions



What Do You Actually Do About It?

Have you ever deleted an app over privacy concerns? Used incognito mode? Given a fake name to protect yourself?

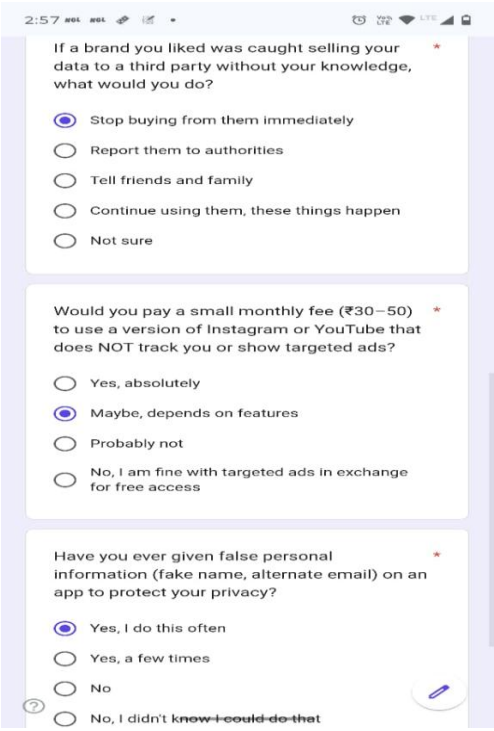
This section looks at real behaviour , not what people say they would do, but what they actually do when they feel their privacy is being invaded.

Which of the following have you done to protect your privacy? (Select all that apply) *

- [x] Turned off mic
- [x] Camera permissions
- [x] Used incognito mode
- [x] Used a VPN
- [ ] Cleared cookies
- [x] Denied app permissions
- [ ] Opted out of personalised ads
- [ ] None of the above

If a brand you liked was caught selling your data to a third party without your knowledge, what would you do? *

- Stop buying from them immediately



2:57

If a brand you liked was caught selling your data to a third party without your knowledge, what would you do? *

- Stop buying from them immediately
- Report them to authorities
- Tell friends and family
- Continue using them, these things happen
- Not sure

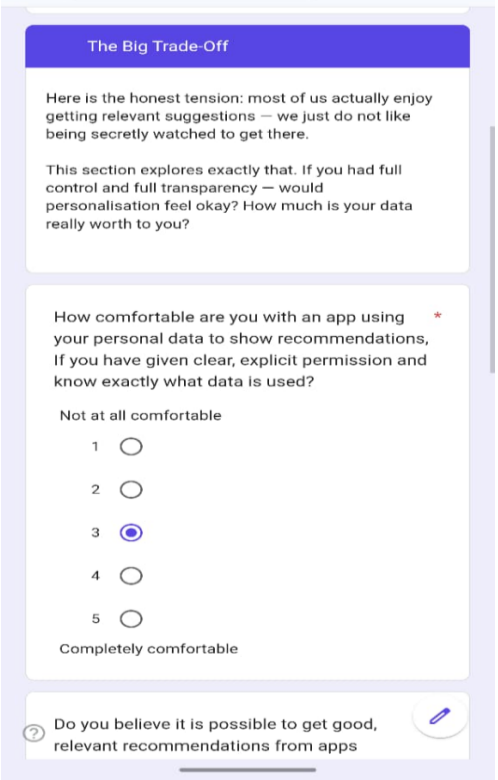
Would you pay a small monthly fee (₹30–50) to use a version of Instagram or YouTube that does NOT track you or show targeted ads? *

- Yes, absolutely
- Maybe, depends on features
- Probably not
- No, I am fine with targeted ads in exchange for free access

Have you ever given false personal information (fake name, alternate email) on an app to protect your privacy? *

- Yes, I do this often
- Yes, a few times
- No
- No, I didn't ~~know I could do that~~

## Section E — Personalization vs. Privacy Trade-Off



The Big Trade-Off

Here is the honest tension: most of us actually enjoy getting relevant suggestions — we just do not like being secretly watched to get there.

This section explores exactly that. If you had full control and full transparency — would personalisation feel okay? How much is your data really worth to you?

How comfortable are you with an app using your personal data to show recommendations, If you have given clear, explicit permission and know exactly what data is used? *

Not at all comfortable

1

2

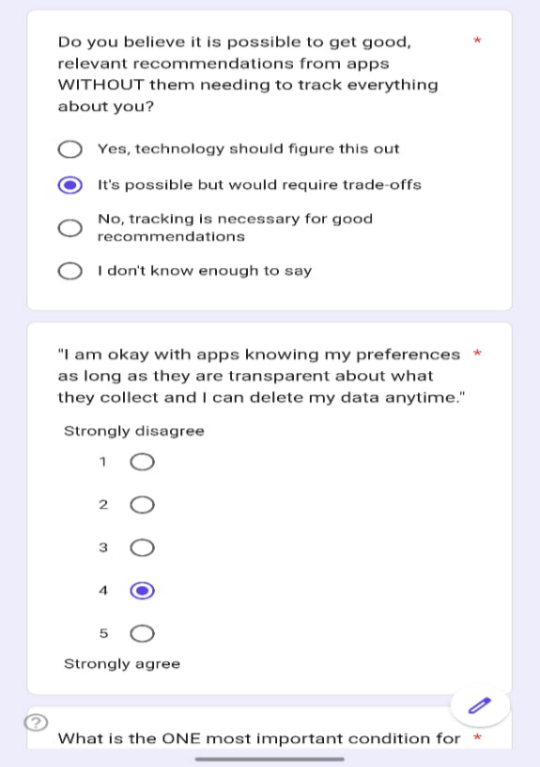
3

4

5

Completely comfortable

Do you believe it is possible to get good, relevant recommendations from apps



Do you believe it is possible to get good, relevant recommendations from apps WITHOUT them needing to track everything about you? *

- Yes, technology should figure this out
- It's possible but would require trade-offs
- No, tracking is necessary for good recommendations
- I don't know enough to say

"I am okay with apps knowing my preferences as long as they are transparent about what they collect and I can delete my data anytime." *

Strongly disagree

1

2

3

4

5

Strongly agree

What is the ONE most important condition for *

| 10% | 9% | 6% | 5% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | Submitted to Delhi Technological University<br>Student Paper | 2% |
| 2 | dspace.dtu.ac.in:8080<br>Internet Source | 1% |
| 3 | link.springer.com<br>Internet Source | <1% |
| 4 | journalofscience.ou.edu.vn<br>Internet Source | <1% |
| 5 | core.ac.uk<br>Internet Source | <1% |
| 6 | studentsrepo.um.edu.my<br>Internet Source | <1% |
| 7 | "Data Mining and Information Security", Springer Science and Business Media LLC, 2026<br>Publication | <1% |
| 8 | Mitchell, Maria. "The Influence of Generational Cohort and Gender on Consumer Perceptions of AI-Driven Personalization in E-Commerce Marketing.", University of Maryland University College<br>Publication | <1% |
| 9 | Submitted to Nanyang Technological University<br>Student Paper | <1% |

| | | |
|---|---|---|
| 10 | Rosa Llamas, Russell Belk. "The Routledge Handbook of Digital Consumption", Routledge, 2022<br>Publication | <1 % |
| 11 | www.theseus.fi<br>Internet Source | <1 % |
| 12 | repository.up.ac.za<br>Internet Source | <1 % |
| 13 | www.cscp.org<br>Internet Source | <1 % |
| 14 | www.ischool.utexas.edu<br>Internet Source | <1 % |
| 15 | Submitted to American Intercontinental University Online<br>Student Paper | <1 % |
| 16 | www.academypublication.com<br>Internet Source | <1 % |
| 17 | Submitted to Indian Institute of Foreign Trade<br>Student Paper | <1 % |
| 18 | repository.iaa.ac.tz:8080<br>Internet Source | <1 % |
| 19 | www.jbdpm.com<br>Internet Source | <1 % |
| 20 | dokumen.pub<br>Internet Source | <1 % |
| 21 | www.coursehero.com<br>Internet Source | <1 % |
| 22 | repository.nwu.ac.za<br>Internet Source | <1 % |

| | | |
|---|---|---|
| 23 | dataforpublicgood.org.in<br>Internet Source | <1 % |
| 24 | ir-library.ku.ac.ke<br>Internet Source | <1 % |
| 25 | Submitted to Kajaanin ammattikorkeakoulu (KAMK)<br>Student Paper | <1 % |
| 26 | repository.unbari.ac.id<br>Internet Source | <1 % |
| 27 | 1library.net<br>Internet Source | <1 % |
| 28 | famt.ac.in<br>Internet Source | <1 % |
| 29 | www.vifindia.org<br>Internet Source | <1 % |
| 30 | mary-ankrah.blogspot.com<br>Internet Source | <1 % |
| 31 | max-cromignon.blogspot.com<br>Internet Source | <1 % |
| 32 | multilogin.com<br>Internet Source | <1 % |
| 33 | pdfs.semanticscholar.org<br>Internet Source | <1 % |
| 34 | rethinkaadhaar.in<br>Internet Source | <1 % |
| 35 | ulspace.ul.ac.za<br>Internet Source | <1 % |
| 36 | americanimpactreview.com<br>Internet Source | <1 % |

| | | |
|---|---|---|
| 37 | ir.vistas.ac.in<br>Internet Source | <1 % |
| 38 | irt.shodhsagar.com<br>Internet Source | <1 % |
| 39 | open.library.ubc.ca<br>Internet Source | <1 % |
| 40 | repository.aaup.edu<br>Internet Source | <1 % |
| 41 | repository.uwtsd.ac.uk<br>Internet Source | <1 % |
| 42 | sciencepg.org<br>Internet Source | <1 % |
| 43 | ul.netd.ac.za<br>Internet Source | <1 % |
| 44 | www.pas.va<br>Internet Source | <1 % |
| 45 | Zou, Yixin. "Understanding and Improving Consumers' Adoption of Online Privacy-Protective Behaviors", University of Michigan, 2023<br>Publication | <1 % |
| 46 | d-nb.info<br>Internet Source | <1 % |
| 47 | e-research.siam.edu<br>Internet Source | <1 % |
| 48 | ijsrem.com<br>Internet Source | <1 % |
| 49 | kipdf.com<br>Internet Source | <1 % |

| | | |
|---|---|---|
| 50 | kwpublications.com<br>Internet Source | <1 % |
| 51 | pure.port.ac.uk<br>Internet Source | <1 % |
| 52 | pureadmin.qub.ac.uk<br>Internet Source | <1 % |
| 53 | releve.erudit.org<br>Internet Source | <1 % |
| 54 | scholar.sun.ac.za<br>Internet Source | <1 % |
| 55 | www.atlantis-press.com<br>Internet Source | <1 % |
| 56 | www.humanitarianlibrary.org<br>Internet Source | <1 % |
| 57 | www.slideshare.net<br>Internet Source | <1 % |
| 58 | Jasmeet Kaur, Abinayarajam D., Rakesh Singh. "Marketing Performance and Factors Influencing Farmers' Choice for Agricultural Output Marketing Channels: The Case of Potato (Solanum tuberosum) in India", Potato Research, 2026<br>Publication | <1 % |
| 59 | Gisela Labouvie-Vief, Manfred Diehl, Lisa M. Chiodo, Nathan Coyle. "Representations of self and parents across the life span", Journal of Adult Development, 1995<br>Publication | <1 % |