How Much Is Data Privacy Worth? A Preliminary Study on WTA and WTP in India

Authors:

Farheen Yousuf, Researcher, Advanced Study Institute of Asia, SGT University

Email: Farheen@advancedstudy.asia

Phone: +91 7095407863

Sahil Amerwal, Research Assistant, Advanced Study Institute of Asia, SGT University

Email: sahilamerwalcontact@gmail.com

Phone: +91 9560412531

Address for correspondence:

Advanced Study Institute of Asia (affiliated to SGT University),

Pocket 5, Sector D, Vasant Kunj, New Delhi, Delhi 110067

Abstract

What is the value of data privacy for Indian consumers? This study examines how much people in India are willing to pay (WTP) to protect their data and how much compensation they would accept (WTA) to give access to it. Replicating a study by Winegar and Sunstein (2019), we find that consumers are willing to pay ₹300 per month to keep their data private but demand ₹3800 to share it. This large gap shows that people value losing privacy much more than gaining it, a pattern called the "superendowment effect." It also highlights challenges like low awareness and lack of information about data use, which make these valuations unreliable for creating laws or policies. In India, where digital knowledge varies widely, relying only on such measures may lead to policies that do not protect consumers effectively.

In India, privacy means different things to different people. Studies show that only 11% of users truly understand privacy risks (Punagin & Arya, 2015). Many trust companies to safeguard their data, even when they don't fully know what happens with it (Dhotre & Olesen, 2015). Married individuals and women are often more careful about privacy, likely because they consider how data use might impact their families or social standing (Kumaraguru & Sachdeva, 2014).

India's Digital Personal Data Protection Act (DPDP), 2023, makes consent a key part of data protection. But consent doesn't work well if people don't fully understand what they are agreeing to. Our study suggests that privacy laws in India need to go beyond just asking for consent. Companies should be made to explain, transparently, how the data is being used and shared. Simultaneously, more awareness campaigns should be carried out to help people make better decisions about their data. Privacy law in India needs to take cognisance of the peculiar interplay of trust, cultural values, and lesser awareness in the country.

Introduction:

Data, in the digital sense, is huge information manufactured and collected by an individual or organisation, even when using various services provided across the internet. It may encompass personal information, names and addresses, social media use, buying patterns, and even health records. This data collection coupled with analysis helps companies know how they can work on their services and marketing techniques to better the user experience and foster business efficiencies[1].

The growing collection of personal data has indeed posed major privacy concerns. Data privacy refers to rights and practices related to proper handling, processing, and storing of personal information. Major privacy concerns are found relating to the growing collection of personal data.[2] Data privacy refers to rights and practices concerning the proper treatment, processing, and storing of personal information. Its significance cannot be underestimated because improper use of personal data can result in severe damage, including identity theft, loss of finances, and erosion in trust over the digital platforms[3].

Angela G. Winegar and Cass R. Sunstein researched consumer concerns over valuing data privacy through a study with 2,416 Americans[4]. They found an astonishing gap between the price that consumers might pay to preserve privacy and what they would charge to lose it. As the report points out, there is a "super endowment effect," wherein the median consumer was willing to pay only $5 a month to preserve data privacy but would charge a whopping $80 to allow access to their data. It is a stark gap and highlights the complications in which cognitive biases operate in relation to data privacy valuation.

Given India's peculiar cultural landscape and the current state of its data privacy laws, similar studies would give precious insights into how much Indian consumers value their personal data,

---

[1] Peter Lake & Paul Crowther, *Data, an Organisational Asset*, in **Organisational Information Systems in the Context of Globalization** 3, 3-19 (2013), https://doi.org/10.1007/978-1-4471-5601-7_1

[2]

[3] Frits W. Hondius, *A Decade of International Data Protection*, 30 **Neth. Int'l L. Rev.** 103, 103-128 (1983), https://doi.org/10.1017/S0165070X00012298

[4] Angela G. Winegar & Cass R. Sunstein, How Much Is Data Privacy Worth? A Preliminary Investigation, 42 J. Consumer Pol'y 425, 426 (2019)

their willingness to protect it, and what the economic implications of potential privacy policies would be. Data privacy in India emerges as one of the outstanding issues that have gained much importance with the emergence of this country as a leader in business process outsourcing.[5] The inflow of personal data from different parts of the world has increased enormously, and hence, their protection and privacy have acquired much importance. This paper builds upon the seminal work of Kumaraguru and Cranor (2005), which examined privacy attitudes and awareness within India's high-tech workforce during the early stages of digital adoption. At that time, their findings highlighted the limited understanding of privacy rights among Indian users and a cultural backdrop that prioritised collectivist values over individual privacy. However, with the advent of widespread internet access and the exponential rise in digital service usage, there is a pressing need to revisit these issues to reflect the shifting technological and legal landscape.

Further, Angela G. Winegar and Cass R. Sunstein's (2019) investigation into the superendowment effect in the American context provides the methodological foundation for this research. Their study revealed stark disparities between consumers' willingness to pay (WTP) to protect their data and their willingness to accept (WTA) compensation for sharing it, a gap explained by behavioural biases such as loss aversion and moral outrage. By replicating and adapting this framework in the Indian context, this paper aims to uncover how cultural and economic factors influence these valuations and whether similar behavioural patterns are evident.

In recent years, India has experienced significant growth in internet usage and digital connectivity. As of January 2024, there were approximately 751.5 million internet users in the country, representing an internet penetration rate of 52.4%.[6] Despite this progress, a substantial portion of the population remains offline, highlighting the ongoing need for digital literacy initiatives. The government has implemented several programs to bridge the digital divide. Notably, the Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) aims to make one person per rural household digitally literate. As of early 2022, approximately 4.9 crore individuals had been trained under this scheme, with around 3.62 crore receiving certification[7]

[5] Ponnurangam Kumaraguru & Lorrie Faith Cranor, Privacy in India: Attitudes and Awareness, in Int'l Workshop on Privacy Enhancing Techs. 243, 243–44 (2005)

[6] DataReportal, Digital 2024: India (Jan. 2024), https://datareportal.com/reports/digital-2024-india.

[7] Ministry of Electronics & Info. Tech., Pradhan Mantri Gramin Digital Saksharta Abhiyan, https://www.pmgdisha.in/

Even with such regulatory efforts, how much do consumers value their data privacy? Studies show that the willingness of consumers to pay for protecting their privacy and what they would claim in consideration for surrendering it are often grossly disproportionate. This suggests that the valuation of data privacy is a complex task and that its real value to consumers is uncertain.

Finally, this study contributes to the literature on data privacy valuation by considering contemporary challenges such as the Digital Personal Data Protection Act (2023), evolving consumer attitudes post-TikTok ban, and India's growing digital economy[8]. Unlike the broader theoretical discussions of data privacy regulations and global trends addressed by prior studies, this paper situates these concerns within India's unique socio-cultural, economic, and regulatory environment, offering an updated perspective that incorporates behavioural economics insights and empirical evidence from recent data.

Experimental Design:

To investigate how Indians value their personal data, we conducted a simple stated-preference survey, replicating the methodology of the US-based study, *"How Much Is Data Privacy Worth? A Preliminary Investigation"* by A. G. Winegar and C. R. Sunstein, with adaptations for the Indian context.[9] Unlike the original study, where respondents were randomly assigned one primary question, our design presented all eight primary questions to each respondent. This approach allowed for comprehensive data collection across various scenarios related to willingness to accept (WTA) and willingness to pay (WTP).

Each respondent answered all eight questions, which varied in the type of personal data involved and whether the question focused on allowing access (WTA) or deleting data (WTP). The questions were presented in a random order, and respondents were then asked follow-up contextual and demographic questions.

The eight primary questions explored WTA and WTP for different categories of personal data:

---

[8] Ministry of Electronics & Info. Tech., Digital Personal Data Protection Act, 2023, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[9] Angela G. Winegar & Cass R. Sunstein, How Much Is Data Privacy Worth? A Preliminary Investigation, 42 J. Consumer Pol'y 425, 426 (2019)

1. **Baseline WTA**: For what amount (in Indian Rupees) per month would you be willing to allow all companies (e.g., Facebook, Google, Flipkart, Paytm) to access your general personal data?
2. **Specific WTA – Personal Information**: For what amount (in Indian Rupees) per month would you be willing to allow all companies to access your data (name, age, gender, profession, household income, address, picture)?
3. **Specific WTA – Sensitive Attributes**: For what amount (in Indian Rupees) per month would you be willing to allow all companies to access your data (age, gender, political affiliation, religion, caste)?
4. **Specific WTA – Health Information**: For what amount (in Indian Rupees) per month would you be willing to allow all companies to access your health data (e.g., physical and mental health, chronic diseases)?
5. **Baseline WTP**: What would you be willing to pay per month (in Indian Rupees) to delete your general personal data from all companies that hold it?
6. **Specific WTP – Personal Information**: What would you be willing to pay per month (in Indian Rupees) to delete your data (name, age, gender, profession, household income, address, picture) from all companies?
7. **Specific WTP – Sensitive Attributes**: What would you be willing to pay per month (in Indian Rupees) to delete your data (age, gender, political affiliation, religion, caste) from all companies?
8. **Specific WTP – Health Information**: What would you be willing to pay per month (in Indian Rupees) to delete your data (age, gender, personality traits, physical and mental health) from all companies?

Results:

Of the 184 responses received, 9 reported exceptionally high valuations of data privacy. To address these outliers, we adapted a method from a US-based study that standardised responses using income data. For the Indian context, we recalibrated the threshold to reflect the 90th percentile of income, which provides a more grounded representation of high earners without including extreme outliers. Based on estimates from the World Inequality Lab's 2022–23 report,

the 90th percentile of income in India is approximately INR 1.2 million annually (INR 100,000 per month). Responses exceeding this threshold were capped at INR 100,000 per month to ensure consistency and comparability. This adjustment balances the need to manage extreme values while maintaining contextual relevance, enabling a robust analysis of data privacy valuations within the Indian framework.

The updated summary statistics with the capped outliers (₹100,000 per month) are presented in Table 2 in the Appendix. This adjustment ensured that extreme valuations did not disproportionately influence the results.

Demographic data of respondents are summarised in Tables 3, 4, and 5 in the Appendix. The sample included a balanced representation of genders, with 59% identifying as female, 41% as male, and 1% preferring not to disclose their gender. Most respondents reported having at least an undergraduate education, with a mean education code of 3.3 (where 3 = Undergraduate). Income was distributed across all categories, with the majority in the ₹3 lakh to ₹6 lakh annual income bracket (mean income code = 2.62).

Respondents were asked about their understanding of data collection and their concern about data privacy. Approximately 58% reported at least a “decent understanding” of data collection, while 42% reported “limited” or “no understanding.” Despite this, more than 70% of respondents expressed being “somewhat concerned” or “very concerned” about the collection of their personal data online. Notably, respondents with a “great understanding” of data collection were more likely to report positive feelings about data collection, compared to those with less understanding. Among respondents with a “great understanding,” 40% expressed “very positive” feelings about data collection, compared to just 15% among those with limited or no understanding.

This suggests that some individuals see benefits in data collection, such as targeted advertising or improved online services, which may outweigh their privacy concerns. However, this could also reflect self-reporting biases, where those who feel positively about data collection are more likely to describe themselves as knowledgeable.

Full summary statistics of WTP and WTA responses can be found in Table 1 in the Appendix. Median and mean valuations (with capped values) are as follows:

Data Category	**WTP Median (₹)**	**WTP Mean (₹)**	**WTA Median (₹)**	**WTA Mean (₹)**
General	300	1,485	3,800	8,209
Personal	350	1,034	3,800	9,492
Sensitive	395	1,099	3,800	10,378
Health	400	1,061	3,825	9,837

WTA values were consistently higher than WTP values across all data types, reflecting an endowment effect. For general data privacy, the median WTA was ₹3,800 per month, compared to a median WTP of ₹300 per month. Similarly, for health data, the median WTA reached ₹3,825 per month, while WTP remained at ₹400 per month.

Variance in responses was significant, particularly for WTA. Standard deviations for WTA ranged from ₹21,034 for general data to ₹24,395 for sensitive data, while WTP standard deviations were smaller, ranging from ₹7,424 to ₹10,390. This variance indicates substantial heterogeneity in respondents' valuations of data privacy, likely reflecting individual differences in perception and context.

It is worth noting that respondents valued sensitive and health-related data privacy higher than general or personal data privacy. For example, median WTA for sensitive data (e.g., identity information) was ₹3,800 per month, with a mean of ₹10,378, compared to ₹8,209 for general data.

Finally, the large variance in responses highlights challenges for policymakers. While median values provide a useful reference, the wide range of responses suggests that individual preferences are diverse and context-dependent. This raises the need for personalised or targeted

privacy policies that account for these differences. Additionally, the significant disparity between WTA and WTP reinforces the importance of educating individuals about data collection practices and their implications, which may influence perceptions and valuations of data privacy.

Discussion: Puzzles and Explanations in an Indian Context

These findings leave two primary puzzles: first, the stark disparity between WTP and WTA for data privacy in India; second, the role of how “personal data” is described and culturally perceived.

A Superendowment Effect, Culturally Amplified

Globally, differences between WTP and WTA are well-documented, often attributed to the "endowment effect"[10]. The typical WTA:WTP ratio for tangible goods like mugs or tickets is about 2:1, while environmental goods like clean air see larger ratios, sometimes reaching 10:1[11]. These gaps are often tied to emotional factors like moral outrage over environmental harm[12]. The **14:1 ratio observed here** for privacy in India represents an extraordinary “superendowment effect,” suggesting an amplified valuation of privacy.

However, the Indian context adds unique layers. Cultural norms, such as collectivism, traditionally place less emphasis on individual privacy compared to the West[13]. Yet, when privacy is reframed as a matter of dignity or sovereignty, as evidenced in public responses to events like the TikTok ban, Indians demonstrate strong resistance to violations of privacy[14]. This duality likely explains the high WTA: privacy is not just a transactional good but a deeply symbolic asset tied to personal and national identity. Furthermore, the moral outrage expressed in

[10] Daniel Kahneman et al., Experimental Tests of the Endowment Effect and the Coase Theorem, 98 J. Pol. Econ. 1325 (1990)
[11] Ronald Cummings et al., Measuring Environmental Values: A Test of the Contingent Valuation Methodology, 89 Am. Econ. Rev. 865 (1986)
[12] Shane Frederick et al., Self-Control and the Regret of Indulgence, 2 Persp. Psychol. Sci. 127 (2009)
[13] Li, Y. Cross-Cultural Privacy Differences, in Modern Socio-Technical Perspectives on Privacy 335 (Bart P. Knijnenburg et al. eds., 2022), https://doi.org/10.1007/978-3-030-82786-1_12
[14] Mishra et al., TikTok Politics: Tit for Tat on the India-China Cyberspace Frontier, 16 Int’l J. Comm. 292 (2022)

high WTA figures aligns with findings by Frederick et al. (2009), who noted that consumers often overstate compensation demands for goods they view as essential to their dignity[15].

What Explains Low WTP?

The low WTP for privacy (e.g., INR 400 or less per month in many cases) is striking. One explanation may be that people perceive privacy as a default right, something they should not have to pay for. Additionally, the concept of paying for privacy may feel alien in a country where digital services are largely free, supported by ad-based revenue models[16]. Loss aversion also plays a role: if the starting point is free privacy, even small costs feel like an unfair demand, triggering protest responses[17].

Economic constraints further exacerbate the low WTP. In a country where disposable income is limited, individuals prioritise immediate needs like food or education over abstract benefits like privacy. This prioritisation aligns with studies indicating that privacy awareness often lags in low-income and rural populations, where the benefits of privacy protections are less tangible[18]. The **digital divide** also complicates matters; rural and economically disadvantaged populations have limited understanding of data privacy, let alone its monetary valuation.

Moreover, the concept of **free-rider effects** may be at play. Individuals may expect the government or large corporations to bear the cost of privacy protections, as these entities are perceived as both beneficiaries of data collection and responsible for safeguarding it. This expectation diminishes the perceived personal cost of ensuring privacy[19].

Understanding High WTA

The WTA numbers, in contrast, reflect strong resistance to parting with privacy. Respondents may be expressing moral outrage, signalling that their dignity is not for sale, rather than making a calculated decision about the utility of their data. This aligns with Frederick's (2013)

---

[15] Shane Frederick et al., Self-Control and the Regret of Indulgence, 2 Persp. Psychol. Sci. 127 (2009)
[16] Angela G. Winegar & Cass R. Sunstein, How Much Is Data Privacy Worth? A Preliminary Investigation, 42 J. Consumer Pol'y 425 (2019)
[17] Andrew Caplin & John Leahy, Psychological Expected Utility Theory and Anticipatory Feelings, 116 Q. J. Econ. 55 (2001)
[18] Banerjee & Duflo, Poor Economics: A Radical Rethinking of the Way to Fight Global Poverty (2011)
[19] Cass R. Sunstein, The Value of Privacy, 93 Minn. L. Rev. 92 (2008)

suggestion that high WTA reflects a symbolic stand rather than an informed valuation of welfare effects.

The term “personal data” evokes different responses based on what it represents. In India, sensitive information like health records, caste affiliations, or marital status carries greater social stigma and is more likely to inflate WTA. By contrast, less personal data, such as age or city of residence, is often seen as inconsequential, mirroring patterns observed globally[20]. However, trust deficit with institutions might add complexity. People may demand higher compensation for disclosing data if they believe it will be misused, particularly by foreign corporations or unregulated platforms. This mistrust stems from high-profile data misuse scandals and the growing perception that data collected by foreign entities poses risks to national security[21].

A central challenge is the lack of consumer information about data practices. The majority of respondents in India are unaware of what data is collected or how it is used, mirroring findings from global studies[22]. This gap in understanding makes it difficult for people to make informed tradeoffs, even when they claim to value privacy. Awareness campaigns such as those launched in Europe during the implementation of the GDPR highlight the role of education in improving privacy valuations. Such efforts are critical for India as the Digital Personal Data Protection Act (2023) comes into force.

Behavioural biases further distort valuation. Present bias leads individuals to undervalue future risks of privacy loss, focusing instead on immediate benefits like free internet access. Unrealistic optimism may also play a role, with people assuming that data breaches will not affect them personally[23]. These biases are magnified in contexts where digital literacy is low and the implications of privacy breaches are poorly understood.

Standard economic theory assumes that individuals make rational tradeoffs, weighing the costs and benefits of disclosing personal data[24]. However, the Indian context complicates this assumption. First, low digital literacy and economic constraints limit the ability of users to make

[20] Alessandro Acquisti et al., What Is Privacy Worth?, 42 J. Legal Stud. 249 (2013)
[21] Mishra et al., TikTok Politics: Tit for Tat on the India-China Cyberspace Frontier, 16 Int’l J. Comm. 292 (2022)
[22] same as 20
[23] Tali Sharot, The Optimism Bias: A Tour of the Irrationally Positive Brain (2012)
[24] George J. Stigler, An Introduction to Privacy in Economics, 6 J. Pol. Econ. 623 (1980)

informed decisions[25]. Second, trust in platforms and institutions remains low, with concerns over government surveillance and corporate misuse of data adding to the perceived costs of disclosure[26].

The superendowment effect observed here challenges the notion that consumers are making rational tradeoffs in India. Instead, privacy valuation appears to be influenced by symbolic reasoning (e.g., privacy as a right or dignity) and cultural mistrust. This symbolic dimension is evident in public debates over privacy issues, where moral and ethical arguments often overshadow utilitarian considerations[27].

Conclusion

The replication study highlights a lower but still significant WTA:WTP ratio (14:1) in India, reflecting the unique interplay of economic, cultural, and behavioural factors. While the superendowment effect is evident, its magnitude is tempered by India's collectivist norms, economic constraints, and limited privacy awareness. These findings underscore the importance of contextualising privacy policies and interventions to address the specific challenges and opportunities in the Indian digital landscape.

India's recently drafted Digital Personal Data Protection Act (2025) is a step forward. However, policymakers must recognise that consumers' privacy preferences are endogenous to the policy environment.

[25] Banerjee & Duflo, supra
[26] Cass R. Sunstein, supra
[27] Shane Frederick et al., supra

Appendix:

1. **Table 1: Summary of Responses (Unstandardized)**

   This table summarises the unstandardized values for willingness to accept (WTA) and willingness to pay (WTP) across all categories of data. Outliers above ₹100,000 were capped.

Category	**Median WTA**	**Mean WTA (SD)**	**Median WTP**	**Mean WTP (SD)**
General Personal Data	₹3,800	₹8,208.57 (21,034)	₹300	₹1,485.11 (10,390)
Personal Information Data	₹3,800	₹9,491.93 (25,519)	₹350	₹1,034.19 (7,424)
Sensitive Identity Data	₹3,800	₹10,378.39 (24,396)	₹395	₹1,099.18 (7,428)
Health Data	₹3,825	₹9,836.79 (23,447)	₹400	₹1,060.63 (7,401)

2. **Table 2: Summary of Responses (Standardized at Max = ₹100,000, Min = ₹0)**

Percentile	**WTA General Personal Data**	**WTP General Personal Data**

1%	₹0	₹0
5%	₹0	₹0
10%	₹100	₹5
25%	₹2,700	₹62.5
50%	₹3,800	₹300
75%	₹4,600	₹500
90%	₹5,000	₹750
95%	₹20,000	₹1,000
99%	₹100,000	₹100,000

3. **Table 3: Demographics (Gender, Age)**

Gender	**Count**	**Percentage**
Male	109	59.24%
Female	74	40.22%
Prefer not to say	1	0.54%

Age Group	Count	Percentage
21–30	73	39.67%
31–40	98	53.26%
41–50	8	4.35%
51–60	5	2.72%
61 and above	0	0.00%

4. **Table 4: Demographics (Income)**

Income Range	Count	Percentage
Up to ₹3 lakh	15	8.33%
₹3 lakh to ₹6 lakh	35	19.44%
₹6 lakh to ₹15 lakh	107	59.44%
Above ₹15 lakh	24	13.33%

5. **Table 5: WTP Linear Regression**

   The omitted categories are women, aged 21–30, with undergraduate education and incomes between ₹3–6 lakh.

Variable	Coefficient	Std. Error	t	p-value
Income Code	-₹240.64	₹259.60	-0.93	0.355
Male (Gender)	-₹179.64	₹106.17	-1.69	0.094
Postgraduate Education	-₹539.53	₹183.63	-2.94	0.004
Understanding Code (Great)	-₹57.85	₹79.07	-0.73	0.466
Attitude Code (Very Positive)	₹69.45	₹90.89	0.76	0.446

6. **Table 6: WTA Linear Regression**

   The omitted categories are women, aged 21–30, with undergraduate education and incomes between ₹3–6 lakh.

Variable	Coefficient	Std. Error	t	p-value

Income Code	₹2,605.19	₹1,653.37	1.58	0.118
Male (Gender)	-₹1,608.34	₹2,499.47	-0.64	0.521
Postgraduate Education	₹5,981.07	₹4,322.82	1.38	0.169
Understanding Code (Great)	₹2,718.51	₹1,861.46	1.46	0.147
Attitude Code (Very Positive)	-₹1,491.50	₹1,257.96	-1.19	0.238

7. **Table 7: Concern About Data Collection vs Understanding (% Respondents)**

Understanding of Data Collection	**Very Concerned**	**Somewhat Concerned**	**No Concern**
No Understanding	100%	0%	0%
Some Understanding	70%	25%	5%
Great Understanding	40%	50%	10%