International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

# Digital Privacy in the Age of Social Media: Awareness, Risks, and Responsible Digital Behaviour Among Youth and Parents in India

**H E Vishruth Gupta, Akshay P**
Department of Computer Applications
BMS College of Commerce and Management, Bengaluru, India
Guide: Asst. Prof. Shrinkhala Kumari

***Abstract***—The rapid proliferation of smartphones and social media platforms has fundamentally altered how individuals across generations interact with digital technology. In India, with over 500 million smartphone users and one of the world's largest active social media populations, digital privacy awareness has emerged as a critical concern. This paper investigates the levels of digital privacy awareness among Generation Z (ages 15–25) and their parents (ages 40–60) in urban Indian contexts, examines prevalent cyber threats targeting both groups, and analyses the behavioural gap between stated privacy concerns and actual digital behaviour—widely termed the 'Privacy Paradox.' Using a mixed-method approach combining survey analysis of 200 respondents, secondary data from CERT-In cybercrime reports, NCRB statistics, and peer-reviewed literature, the study reveals that Gen Z users exhibit high digital fluency but demonstrate significant privacy risk behaviour, while older adults face disproportionate targeting by financial cyber fraud despite lower digital engagement. The paper proposes the Family Digital Literacy Model (FDLM) as a community-based intervention and discusses policy implications for educational institutions, technology platforms, and government agencies.

***Keywords***—digital privacy; cybersecurity awareness; social media; Generation Z; family digital literacy; cyber fraud; India; data protection; online safety

## I. INTRODUCTION

In the contemporary digital ecosystem, privacy is no longer confined to physical boundaries—it is an active, continuous negotiation between individual users and technology platforms. The smartphone has evolved into a comprehensive personal data repository, capturing behavioural patterns, locational data, communication histories, financial transactions, and social interactions in real time. The aggregation of this data forms the 'digital identity'—simultaneously more detailed and more vulnerable than its physical counterpart.

India presents a uniquely compelling case study for digital privacy research. According to the Telecom Regulatory Authority of India (TRAI), India had approximately 540 million active internet users as of early 2026, with social media penetration estimated at over 60% of the urban population [1]. The Indian Computer Emergency Response Team (CERT-In) reported cybercrime losses exceeding ₹11,000 crore in 2023, with financial fraud, phishing, and identity theft constituting the majority of cases [2].

This study situates itself at the intersection of two critical social phenomena: (1) the growing primacy of social media in the lives of Indian youth, and (2) the expanding but under-prepared digital presence of an older generation navigating online environments without adequate preparedness. The central research question is: What is the nature and extent of the digital privacy awareness gap between Generation Z and their parents in urban India, and how can intergenerational learning bridge it?

The remainder of this paper is organized as follows: Section II reviews relevant literature. Section III states the research objectives. Section IV describes the methodology. Section V presents findings and analysis. Section VI discusses implications. Section VII proposes the Family Digital Literacy Model. Section VIII offers recommendations, and Section IX concludes the paper.

## II. LITERATURE REVIEW

### *A. The Privacy Paradox*

The 'Privacy Paradox'—first articulated by Barnes [3] and expanded by Acquisti and Grossklags [4]—describes the phenomenon wherein individuals express concern about online privacy while engaging in behaviours that undermine it.



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Norberg, Horne, and Horne demonstrated through controlled experiments that users consistently disclose more personal information than their stated preferences suggest, attributing this to hyperbolic discounting: the tendency to value immediate gratification over long-term privacy consequences [5]. This paradox is consistently observed in global studies and is particularly pronounced among high-frequency social media users.

*B. Digital Privacy and Adolescent Behaviour*

Livingstone conducted extensive research on European youth and digital risk, concluding that teenagers possess digital skills that far outpace their digital safety awareness [6]. Madden et al. in a Pew Research Center survey found that while 60% of American teenagers claimed to value online privacy, over 90% had posted personal photographs publicly [7]. In the Indian context, Kaur and Nayak surveyed 1,200 students across Bengaluru and Delhi, finding that 84% had never reviewed app permissions, despite 72% expressing concern about data misuse [8].

*C. Vulnerability of Older Adults in Digital Spaces*

Lichtenberg et al. highlight the disproportionate targeting of older adults by cybercriminals, identifying cognitive vulnerability, lower digital confidence, and social isolation as compounding risk factors [9]. In the Indian context, Sharma and Mahesh conducted field studies in Bengaluru, Pune, and Hyderabad, finding that adults aged 50 and above were 2.3 times more likely to fall victim to financial cyber fraud than younger adults, primarily through WhatsApp-based scams and fraudulent UPI payment requests [10].

*D. The Role of Family in Digital Literacy*

Research by Shin and Lwin indicates that parental mediation significantly reduces risky online behaviour in adolescents [11]. However, the traditional top-down model of parental mediation becomes inadequate when parents themselves lack digital competence. Researchers increasingly advocate for a bidirectional digital literacy model, wherein knowledge flows between generations [12], [13].

*E. Regulatory Framework in India*

The Digital Personal Data Protection Act (DPDPA), passed in August 2023, establishes consent-based data processing and creates obligations for Data Fiduciaries [14]. However, Ramanathan notes significant implementation gaps, particularly regarding user awareness of rights available under the Act [15].

## III. RESEARCH OBJECTIVES

The study pursues the following specific objectives:

1. To assess the level of digital privacy awareness among Indian youth (Gen Z) and their parents.
2. To identify the most common digital privacy risks and cyber threats faced by each demographic.
3. To examine the behavioural gap between stated privacy concerns and actual digital behaviour.
4. To explore how intergenerational knowledge exchange within families can serve as a practical digital safety mechanism.
5. To propose evidence-based recommendations for educational institutions, families, and technology platforms.

## IV. RESEARCH METHODOLOGY

*A. Research Design*

This study adopts a mixed-method research design, combining quantitative survey data with qualitative secondary analysis. The mixed-method approach is chosen to capture both the measurable dimensions of digital behaviour and the nuanced, context-dependent nature of privacy decision-making.

*B. Primary Data Collection*

A structured questionnaire comprising 30 items was administered to two participant groups in the Bengaluru metropolitan area. The survey was distributed digitally via Google Forms to student respondents and in printed form to parent respondents to mitigate digital access bias.

- Group A (Gen Z): 120 students aged 15–25, enrolled in pre-university and undergraduate programmes.
- Group B (Parents): 80 adults aged 40–60, identified as parents or guardians of Group A respondents.
- Total sample: 200 participants across 6 institutions in Bengaluru.

*C. Secondary Data Sources*


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Secondary data was drawn from: CERT-In Annual Cybercrime Reports (2021–2024) [2]; Pew Research Center Digital Privacy Surveys [7]; Internet and Mobile Association of India (IAMAI) Digital Adoption Reports 2024 [16]; National Crime Records Bureau (NCRB) Cyber Crime Statistics 2023 [17]; and India's Digital Personal Data Protection Act, 2023 [14].

### *D. Limitations*

The sample is geographically limited to urban Bengaluru and may not represent rural or semi-urban Indian populations. Self-reported survey data is subject to social desirability bias. The study is cross-sectional and does not capture longitudinal changes in digital behaviour.

## V. FINDINGS AND ANALYSIS

### *A. Digital Behaviour of Gen Z Respondents*

Survey findings reveal that Gen Z respondents spend an average of 6.2 hours per day on digital devices, with social media constituting approximately 3.5 hours of that usage. Instagram, YouTube, and WhatsApp are the three most-used platforms, used by 94%, 91%, and 88% of respondents respectively. Despite this high digital engagement, privacy awareness is notably poor:

- 78% had never reviewed privacy settings on their primary social media account.
- 82% clicked 'Allow All' on app permission prompts without reading individual requests.
- Only 23% had Two-Factor Authentication (2FA) enabled on their accounts.
- 67% were unaware that app developers could sell their data to third parties.
- 91% used the same password across multiple platforms.

### *B. Digital Behaviour of Parent Respondents*

Parent respondents showed lower overall digital engagement (average 2.8 hours/day) but demonstrated distinct vulnerability patterns. WhatsApp was used by 97% of parent respondents, making it the dominant platform for this group.

- 63% had forwarded at least one unverified news item on WhatsApp in the past month.
- 41% had clicked on a link from an unknown sender in the past three months.
- 29% reported having received a fraudulent UPI payment request or OTP phishing attempt.
- Only 18% had changed their phone’s default privacy settings since purchase.
- 74% were unaware of India’s Digital Personal Data Protection Act, 2023 [14].

### *C. Common Cyber Threats Identified*

Cross-referencing primary survey data with CERT-In national statistics [2], the following threats were identified as most prevalent:

- Phishing Attacks: Fraudulent messages impersonating banks or government agencies—targeted predominantly at adults over 40.
- Social Engineering Scams: WhatsApp impersonation of family members requesting emergency funds.
- Data Harvesting via Apps: Excessive permission grants enabling silent data collection—most prevalent among 15–25 age group.
- Identity Theft via Oversharing: Publicly accessible personal information enabling targeted fraud.
- OTP Fraud: Vishing calls manipulating users into sharing One-Time Passwords.

### *D. The Privacy Paradox in the Indian Context*

Consistent with global literature [3], [4], [5], the study found a clear Privacy Paradox among both groups. When asked to rate privacy concern on a scale of 1–10, Gen Z respondents averaged 7.4, while parent respondents averaged 6.8—both indicating moderate-to-high concern. However, over 75% of Gen Z and 68% of parent respondents regularly engaged in at least three high-risk digital privacy behaviours simultaneously. This gap between expressed concern and actual behaviour is consistent with hyperbolic discounting theory [5]: immediate convenience consistently overrides abstract privacy concerns.

**TABLE I. SUMMARY OF KEY SURVEY FINDINGS**

| Indicator | Gen Z (n=120) | Parents (n=80) |
|---|---|---|
| Never reviewed privacy settings | 78% | 82% |


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

| | | |
|---|---|---|
| Allow all app permissions without reading | 82% | 54% |
| 2FA enabled | 23% | 9% |
| Unaware data can be sold to 3rd parties | 67% | 81% |
| Shared/forwarded unverified content | 34% | 63% |
| Clicked unknown sender link (last 3 months) | 28% | 41% |
| Aware of DPDPA 2023 | 19% | 26% |

## VI. DISCUSSION

The findings illuminate a fundamental contradiction at the heart of India's digital transition: widespread adoption of digital technologies without a corresponding adoption of digital safety literacy. The challenge is compounded by the simultaneous presence of two demographically distinct groups in the same ecosystem—Gen Z with high fluency but low risk awareness, and older adults with lower fluency who are targeted precisely because of their vulnerability.

Conventional cybersecurity education—directed either at youth in school settings or at older adults through public campaigns—fails to account for the social and relational dimensions of digital behaviour. Digital decisions are rarely made in isolation; they occur within family units, social groups, and community networks [12]. An intervention model that ignores these relational contexts is structurally incomplete.

Platform design also plays a significant role in exacerbating privacy vulnerability. The deliberate burial of privacy settings, dark patterns in consent interfaces, and addictive reward mechanisms create structural conditions that undermine even well-intentioned privacy choices. This suggests that individual-level behavioural change, while necessary, is insufficient as a standalone strategy.

## VII. THE FAMILY DIGITAL LITERACY MODEL (FDLM)

Based on the study's findings and synthesising existing literature [11], [12], [13], this paper proposes the Family Digital Literacy Model (FDLM) as an actionable, community-rooted intervention framework. The FDLM operates on three core principles:

### *A. Bidirectional Knowledge Exchange*

Gen Z family members serve as 'Digital Navigators,' explaining new threats, platform changes, and privacy settings to parents. Parents serve as 'Trust Anchors,' sharing real-world experience about scam patterns, financial decision-making, and social engineering tactics—which closely mirror digital fraud methodologies.

### *B. The Monthly Family Digital Check-In*

A structured 15-minute monthly family conversation is proposed as the primary intervention mechanism. Each session covers: (1) one digital threat encountered in the past month; (2) one practical privacy action taken (e.g., enabling 2FA, revoking app permissions); and (3) one technology update relevant to family members. This low-barrier, habitual approach draws from behaviour change theory [18] and family systems theory [19].

### *C. Institutional Integration*

Educational institutions should formally incorporate the FDLM through: mandatory digital literacy modules (minimum 20 hours per academic year); 'Digital Safety homework' requiring students to conduct family privacy audits; and parent engagement workshops conducted in regional languages to maximise accessibility.

## VIII. RECOMMENDATIONS

### *A. For Individuals and Families*

- Conduct a monthly 'Permission Audit'—review and revoke unnecessary app permissions on all household devices.
- Enable Two-Factor Authentication on all financial, email, and social media accounts.
- Establish a family rule: No OTP, password, or sensitive information is shared over phone or message, regardless of the caller's claimed identity.
- Treat personal data with the same caution as physical financial documents.

### *B. For Educational Institutions*

- Integrate digital privacy as a mandatory standalone subject at secondary and higher secondary levels.
- Develop case-based learning modules drawing from actual Indian cybercrime cases documented by CERT-In [2].


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Create family-inclusive digital literacy programmes delivered in regional languages.

*C. For Technology Platforms*

- Design privacy-by-default interfaces—privacy-protective settings should be the default, not an opt-in.
- Eliminate dark patterns in consent design; provide genuinely equal prominence to 'Accept' and 'Decline' options.
- Provide mandatory plain-language summaries of data collection practices at app installation.

*D. For Government and Policy Makers*

- Accelerate implementation of the Digital Personal Data Protection Act, 2023 [14], with particular attention to enforcement mechanisms.
- Launch a national digital literacy campaign targeting semi-urban and rural populations.
- Mandate cybersecurity awareness training for financial service providers directed at elderly customers.

## IX. CONCLUSION

This research has established that digital privacy in India is not merely a technological challenge—it is a social, educational, and generational one. Gen Z users, despite superior digital fluency, demonstrate a consistent Privacy Paradox: high concern about privacy in principle, low protective behaviour in practice. Older adults face disproportionate exposure to financial cyber fraud enabled by systemic knowledge gaps.

The most promising pathway toward meaningful digital safety is relational: the cultivation of intergenerational, family-centred digital literacy habits that leverage the complementary strengths of both Gen Z's technological familiarity and older adults' accumulated social wisdom. The proposed Family Digital Literacy Model (FDLM) represents a practical, low-cost, and culturally resonant framework for implementing such habits.

As India continues to build its digital infrastructure, the question of who benefits from that infrastructure—and who is left exposed by it—will be determined not by the speed of connectivity, but by the depth of awareness. Digital India must also mean Digitally Safe India.

## ACKNOWLEDGMENT

The authors express sincere gratitude to Asst. Prof. Shrinkala Kumari for her invaluable guidance and mentorship throughout this research. The authors also acknowledge BMS College of Commerce and Management, Bengaluru, for providing the academic environment and institutional support that made this study possible. Special thanks are due to all student and parent respondents who participated in the survey.

## REFERENCES

[1] Telecom Regulatory Authority of India (TRAI), "Telecom Subscription Data—December 2025," Government of India, 2025.
[2] Indian Computer Emergency Response Team (CERT-In), "Annual Report on Cybersecurity Incidents in India 2023–2024," Ministry of Electronics and Information Technology, New Delhi, 2024.
[3] S. B. Barnes, "A privacy paradox: Social networking in the United States," First Monday, vol. 11, no. 9, Sep. 2006.
[4] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," IEEE Security & Privacy, vol. 3, no. 1, pp. 26–33, Jan.–Feb. 2005.
[5] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," Journal of Consumer Affairs, vol. 41, no. 1, pp. 100–126, 2007.
[6] S. Livingstone, "Developing social media literacy: How children learn to interpret risky opportunities on social network sites," Communications: The European Journal of Communication Research, vol. 39, no. 3, pp. 283–303, 2014.
[7] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton, "Teens, Social Media, and Privacy," Pew Research Center, Washington, D.C., May 2013.
[8] P. Kaur and S. Nayak, "Digital literacy and privacy awareness among Indian youth: A survey-based study," Journal of Information Science and Technology, vol. 18, no. 2, pp. 44–61, 2021.
[9] P. A. Lichtenberg, L. Stickney, and D. Paulson, "Is psychological vulnerability related to the experience of fraud in older adults?" Clinical Gerontologist, vol. 36, no. 2, pp. 132–146, 2020.
[10] R. Sharma and K. Mahesh, "Cyber fraud vulnerability among elderly adults in urban India: Patterns, risk factors, and implications," Indian Journal of Criminology, vol. 50, no. 1, pp. 75–93, 2022.
[11] W. Shin and M. O. Lwin, "How does asking about Internet use relate to parental mediation of children's online activities?" Computers in Human Behavior, vol. 72, pp. 229–239, 2017.
[12] L. S. Clark, "Parental mediation theory for the digital age," Communication Theory, vol. 21, no. 4, pp. 323–343, 2011.
[13] M. Ito, S. Baumer, M. Bittanti, d. boyd, and R. Cody, Hanging Out, Messing Around, and Geeking Out: Kids Living and Learning with New Media. Cambridge, MA: MIT Press, 2020.
[14] Ministry of Electronics and Information Technology (MeitY), "The Digital Personal Data Protection Act, 2023," Government of India, Official Gazette, Aug. 2023.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

[15] U. Ramanathan, "The DPDP Act and the gap between law and implementation: A critical review," Economic and Political Weekly, vol. 59, no. 3, pp. 18–24, 2024.
[16] Internet and Mobile Association of India (IAMAI), "India Internet Report 2024," IAMAI & Kantar, Mumbai, 2024.
[17] National Crime Records Bureau (NCRB), "Crime in India 2023: Statistics—Cybercrime," Ministry of Home Affairs, Government of India, New Delhi, 2023.
[18] B. J. Fogg, Tiny Habits: The Small Changes That Change Everything. New York, NY: Houghton Mifflin Harcourt, 2019.
[19] M. Bowen, Family Therapy in Clinical Practice. New York, NY: Jason Aronson, 1978.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)