Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Digital Privacy Laws – Evolution and Consumer Perceptions among online users in India

Article History:

Name of Author:
Dr. Priya Harikumar[1], Dr. Jayashree Balasubramanian[2], Dr. Sumitra Padmanabhan[3], Prof. Amit Bathia[4], Dr. Kajal Chheda[5], Dr. Kavita Nikam[6]

Affiliation:
[1]*Associate Professor, ATLAS Skilltech University, Mumbai*
[2]*Assistant Professor, ATLAS Skilltech University, Mumbai*
[3]*Associate Professor, ATLAS Skilltech University, Mumbai*
[4]*Assistant Professor, ATLAS Skilltech University, Mumbai*
[5]*Associate Professor, ATLAS Skilltech University, Mumbai*
[6]*Assistant Professor, ATLAS Skilltech University, Mumbai.*

Corresponding Author:
Prof. Amit Bathia

***Email**: amit.bathia@atlasuniversity.edu.in* .

How to cite this article:
Harikumar P, *et al.* Digital Privacy Laws – Evolution and Consumer Perceptions among online users in India. *J Int Commer Law Technol.* 2025;6(1):427–436.

Received: *27-07-2025*
Revised: *16-08-2025*
Accepted: *16-09-2025*
Published: *30-09-2025*

Abstract: As India rapidly embraces digital technologies, concerns surrounding data privacy and the protection of personal information have become increasingly significant. This study explores the progress of digital privacy laws in India and assesses consumer perceptions and awareness among Indian online users regarding data protection. With the proliferation of internet usage, particularly through social media, digital banking, and mobile applications, individuals are frequently exposed to risks such as impersonation, phishing, romance scams, and data breaches. Notwithstanding the introduction of critical legislative frameworks—including the Information Technology Act (2000), its 2008 amendment, and the Digital Personal Data Protection Act (2023)—public understanding and engagement with these laws remain restricted. To evaluate user awareness, a structured online survey was conducted with 153 respondents from diverse demographic backgrounds. Findings reveal that over 70% of respondents lacked awareness of existing data privacy laws, frequently consented to terms without understanding, and showed uncertainty about their rights and remedies. The study also categorizes key types of cybercrimes prevalent in India and contextualizes them within the broader policy landscape. Challenges such as low digital literacy, complex consent mechanisms, limited outreach, and government surveillance concerns are also addressed.
This paper contributes by tracing India's legislative progress on data privacy, identifying user-level gaps, and offering actionable recommendations to enhance awareness, promote informed consent, and strengthen the digital ecosystem. It concludes by emphasizing the need for a multi-stakeholder approach involving government, industry, and civil society to create a privacy-aware and digitally resilient population. Future research directions are also proposed, focusing on mechanisms for improving transparency, regulatory adaptation, and consumer empowerment in the digital age.

Keywords: Digital privacy, consumer perceptions, data privacy laws, cybersecurity, data protection, data protection policies.

INTRODUCTION

In the current digital era, the internet has become an essential part of daily life for millions of Indians, facilitating communication, education, commerce, and entertainment. However, with the rapid increase in online activities, anxiety regarding data privacy and the safety of personal information have emerged. Indian online users often share vast amounts of sensitive data across several platforms, including social media, e-commerce websites, and mobile

applications. Yet, awareness regarding how this information is utilized, shared, and potentially exploited remains alarmingly low among many users. This gap in knowledge exacerbates vulnerabilities, making individuals susceptible to privacy breaches, identity theft, and various forms of cybercrime.

Given the significant rise in internet penetration and the adoption of smartphones in India, the importance of fostering an informed online user base cannot be overstated. Recent studies indicate that while user's express concerns over privacy, most lack a solid understanding of data protection principles and the legal frameworks in place, such as the Information Technology Act and the recently proposed Personal Data Protection Bill.

Our focus here is on the social media related attacks and how individuals are prone to those. The issue of internet secrecy in India is a critical concern, reflecting the need for robust policies and bring about awareness amongst users to protect users' personal data online. India's legislative measures for internet privacy include various laws and regulations aimed at safeguarding user information, although there are ongoing debates about their effectiveness and comprehensiveness. Here, we discuss the various data protection policies in India and how various government surveillance practices have raised significant privacy concerns, with calls for more transparency and accountability in monitoring citizens' online activities.

This research paper focuses to explore the below questions

1. What is the level of awareness among Indian online users about data privacy? To answer this, a detailed online was conducted to understand the awareness of laws and vulnerability amongst diverse population.
2. What are the risks associated with sharing personal information, by shedding light on these crucial aspects? We researched and analysed the various associated risks.
3. What are the challenges in enhancing data protection awareness among users to empower them in making informed digital decisions?

We used Internet Privacy and Data privacy policies in India and based on the policies and the online survey findings, suggested a recommendation to enhance awareness amongst users.

LITERATURE REVIEW

Author, Huang (2023)1, examined the ethical implications of using artificial intelligence in educational settings, particularly concerning student data privacy and protection. The authors intended to study the importance of developing clear and ethical policies and frameworks in order to secure and guarantee responsible use of AI technologies in education. The authors Drachsler and Greller (2016)3 announced the "DELICATE" checklist which is a framework to ensure privacy and trust. This would help schools and universities help student data responsibly. and thereby guiding ethical data practices in educational environments.

The ongoing process of integration of digital change is highlighted by taking small steps and course of action in the banking eco system (Lottu et al., 2023)6. An article published in 2024 by Ezeocha2 reviews how digital banking in Nigeria has evolved over the years and how the baning operations has advanced following that and the study also addresses the several opportunities and also the challenges in adapting to a digital ecosystem in banking.

A paper published in 2023 suggests that it is certainly pivotal to robustly save confidentiality and prevent exploitation of data (Allahrakha, 2023)4, the development of digital channels and banks are consistently heading to stored and transfer data (Wewege et al., 2020)5. Although there has been a consistent study on embracing technology and its repercussions in the banking industry (Chaudhry and Hydros, 2023)7, not much is investigated about the challenges of banks in maintaining safe utility of technology.

Although significant progress has been made in critical sectors such as education and finance, raising awareness among general users remains a persistent challenge.

RESEARCH METHODOLOGY

The work was divided into three sections. To check the level of awareness, a comprehensive questionnaire-based survey was conducted, utilizing various channels, including personal email, contacts and LinkedIn to imbibe the level of awareness of Indian web users about data privacy and its implications. Our approach resulted in the collection of 153 responses, which provided a robust dataset for subsequent analysis. The findings derived from this survey will be detailed in the following sections of the research paper.

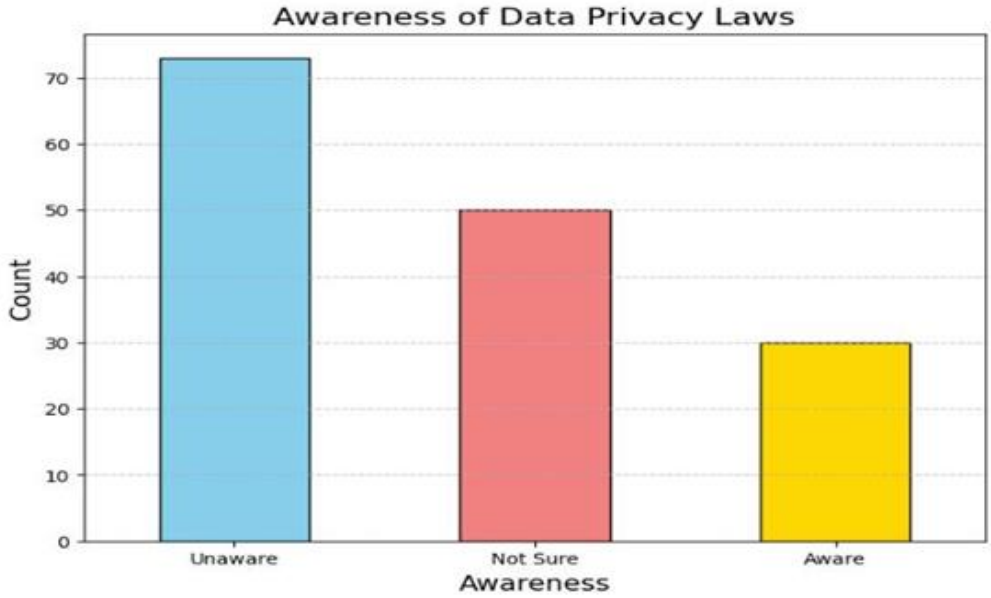
3.1 Level of awareness of Indian customers about the data privacy laws (Based on Questionnaire survey)

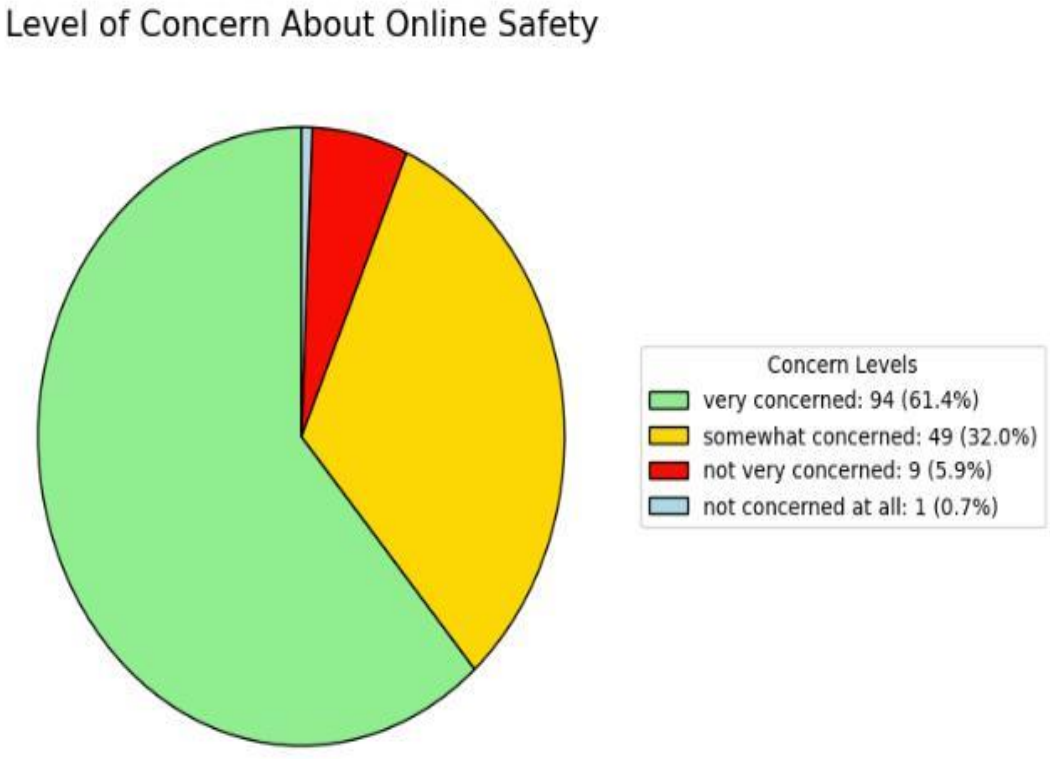
Awareness of Data privacy laws

70% of the respondents were unaware of the data privacy laws, and how it can be mishandled and had instances of suing for the reputational damages caused.

50% were not sure of the policy tick box which they were consenting and always in rush to go to the next page. This way customers are legally abiding and complies by the rules and it protects both the parties the customers and the business. A click wrap agreement is a digital contract which is effective online.

30% were aware of the repercussions, negative consequences which includes lawsuits, loss of customer trust which an individual face. Most data privacy laws have significant fines for non-compliances. The risk can be reduced with robust data privacy measures. Unsanctioned and unwarranted access to personal information can lead to challenges.



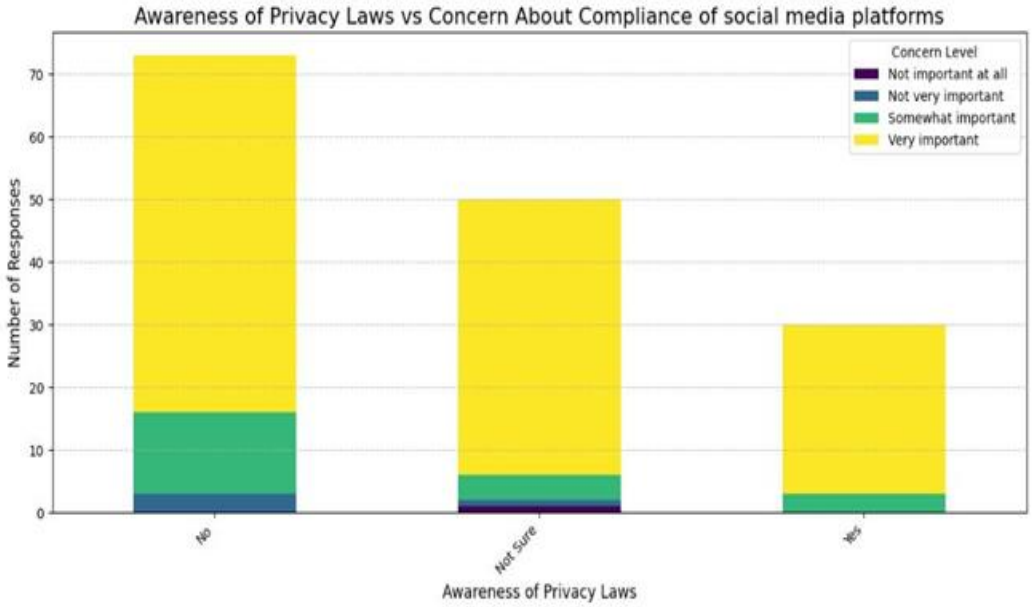


61.4% respondents were very concerned, as companies were collecting and utilizing their personal details as a significant amount was revealed online. There was a fear of data breaches and anonymity is increasingly valued for such customers.

32.0% were somewhat worried, as they were aware of the nuisance, and realised that someone was peering into another in an inquisitive manner. This was affecting the privacy of one's personal sphere.

5.9% respondents were not anxious or disturbed about online safety, they were unbothered and expressed a sense of helplessness.

0.7%1 respondents were not at all restless or panicky, however it is most important to avoid victimisation and manipulation of online fraudsters.



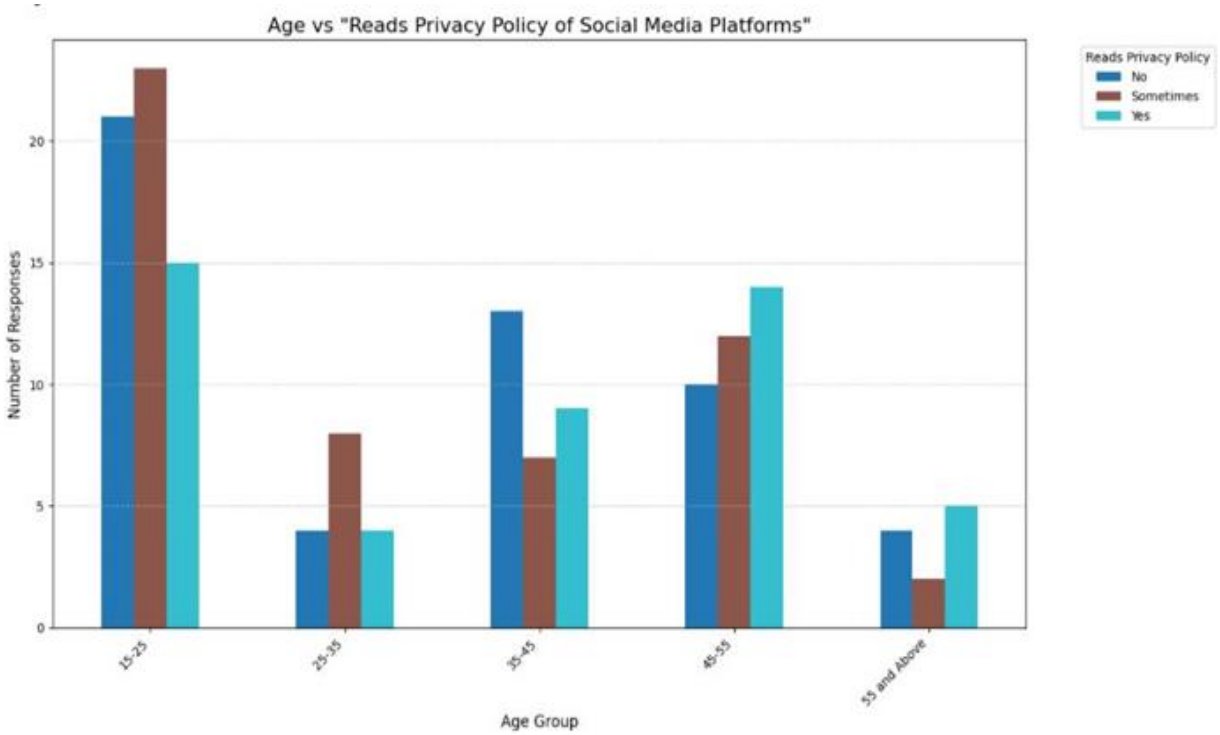
Complying with privacy laws protects businesses and it is important that customer's must understand how the sensitive data is handled in organisations. Although consumers are provided access to correct their own records, social media platforms must mandatorily confirm and abide by clearly intimating the users about the General Data protection regulation.

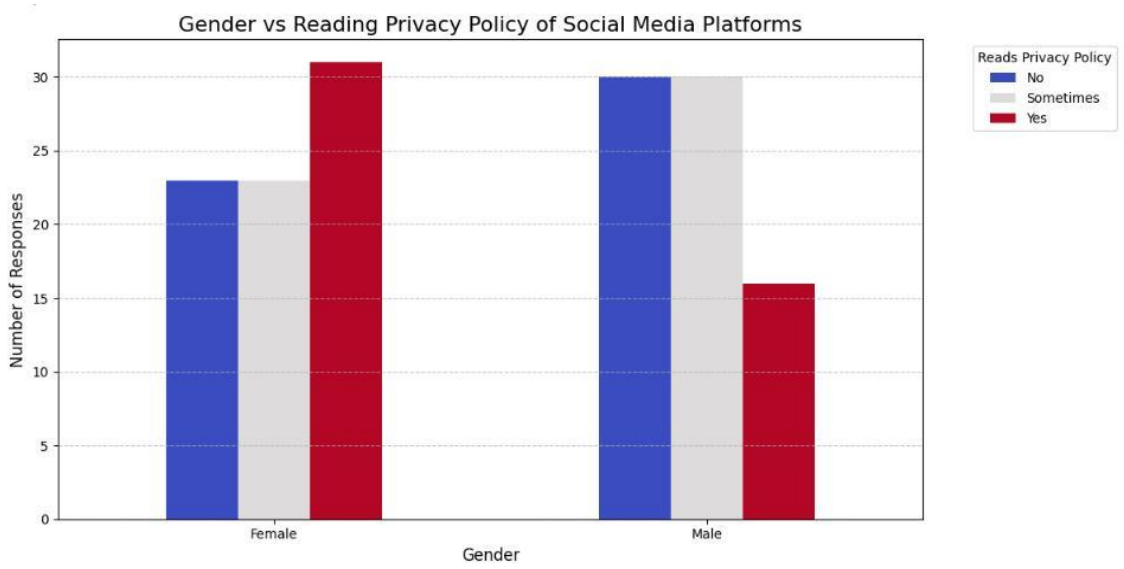
Around 75 % of respondents Very important as compliance and adherence of social media platforms develops an openness and honesty with customers. A feeling of dependability and credibility has to be created between both the platforms.

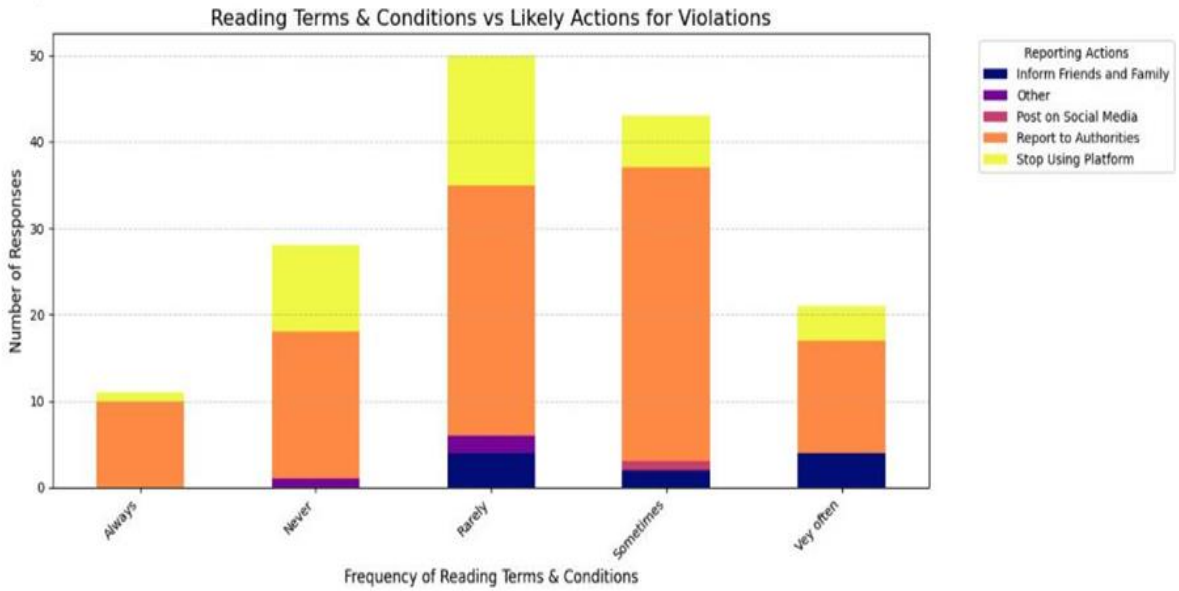
Approximately 15 % feel it is somewhat important as they are not definite of the circumstances and repercussions. Awareness has to be laid out and straightened in social media platforms has it is crucial for individuals.

Roughly 5 % feel it is not very important as they are ignorant and unenlightened, specially the senior citizens who ae unexposed to digital literacy and get compromised due to sweet talk.

About 5% not important at all as it is considered as a myth for the few who do not venture into reading.







3.1.1 Frequency of reading terms and conditions

50% stop using the platform rarely

Use of apps have increased post the pandemic and there is a disconnect between the consumers and the social media. The consumers are unaware about how much information is secure and do not actually read the terms and conditions. The display of the terms of service and terms of use comes only once and the rush to go ahead prevents users in reading it in detail.

38% report to authorities sometimes

Consumer protection laws are supressed as users must seek help from qualified lawyers for sound legal advice. Sometimes disgruntled consumers are afraid to report due to repercussions and threat from external miscreants. Customers publicly share negative experiences, losses and miscreants as apps and other applications policy tick boxes are accepted in a jiffy.

Customers emits and pour out their frustration and emotions in various social media platforms. Unsatisfied users make events viral and public awareness has become contagious across various socio economic and financial status. On the contrary satisfied customers like the company pages, write blogs on social media websites and facilitates the success of the app supports and advocates the interface.

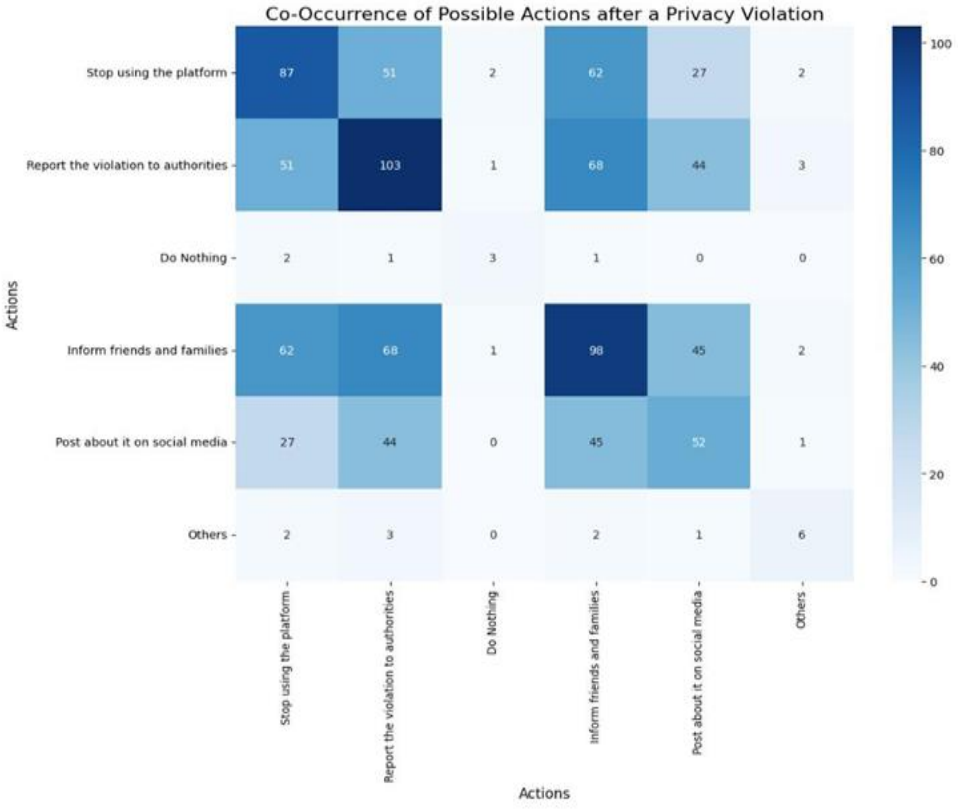
However, companies, vendors and app operators do provide a platform in their website for customer queries, concerns, anxieties, dilemmas and pain points. This enables and equips the customers to continue business in a proactive manner and allow companies to address the relevant issues.

The interface ecosystem sometimes takes advantage of the unknown ignorant.

5% inform friends and family

Customers are frightened to inform friends and relatives as they feel judged and hence hesitate. Many decisions are done secretly and explaining to family is cumbersome. People also feel that since online activities are audited, surveyed, monitored, documented and might malign the reputation of the family. Social stigma prevents individuals from disseminating information as their ignorance could be noticed by family and friends.

Nevertheless, it is less secured then what it was earlier.



Based on the responses collected, which shows 70% respondents are ignorant of Indian data privacy laws, we feel it is important that we increase the awareness of our people on these major issues considering the risks that all are exposed to. So, below we have categorized the various types of cyber frauds and crimes and later explained what laws exist that safe guard our rights and how they evolved over time.

3.2 Multifaceted issues surrounding privacy in the digital era

The section 2 includes discussion risks associated with sharing personal information. Research conducted by Agarwal. A (2023)[10], which explores the multifaceted issues surrounding privacy in the digital era was discussed. Concentration was on the legal, technological, and ethical dimensions. Further, the categories of prevalent cybercrimes as per Government of India (cybercrime.gov.in)[8], were discussed. Some of them included: -

Identity theft

It is a growing concern in the digital age, with individuals increasingly vulnerable to various forms of data breaches and misuse. One of the most common methods includes hacking or unauthorized access to social media accounts, which can direct towards impersonation, monetary fraud, or tarnish. Additionally, the misuse of photocopies of identity proofs, such as Aadhar cards or driver's licenses, poses a serious threat, especially when these documents are shared without proper safeguards. Another widespread technique is credit or debit card skimming, where fraudsters use secret devices to steal card information during righful transactions. Together, these methods highlight the urgent need for greater public awareness and stronger security measures to protect personal information.

Psychological tricks

Cybercriminals often exploit psychological tricks to manoeuvre and orchestrate individuals into revealing sensitive information or making impulsive decisions that lead to fraud. Techniques like phishing, vishing, and smishing use counterfeit emails, calls, or text messages to deceive users into sharing personal or financial details. Lottery scams, fake job offers, and online marketplace frauds lure victims with promises of easy money or discounted deals. Fraudsters also exploit technology by skimming ATM cards, cloning

cards at merchant outlets, or stealing data through public charging cables. QR code scams and search engine manipulation are newer tactics to compromise credentials. Furthermore, many fall prey to charity frauds, fake discounts, unauthorized credit card activations, and fraudulent loan offers. The rise of illegal loan financing apps and Aadhaar-related scams adds to the growing list of threats. These schemes highlight the importance of digital literacy and scepticism when dealing with unsolicited messages or offers, especially when they seem too good to be true.

Social media–related attacks

It encompasses an extensive, comprehensive range of deceptive practices that accomplish the interactive and trust-based nature of social platforms. These attacks have significant financial, emotional, and reputational consequences for victims. Common tactics include cyberstalking, cyberbullying, and romance fraud, where attackers build emotional connections to manipulate individuals. Phishing scams, fake profiles, and credential harvesting leads to access of data breach. Fraudsters also promote fake investment schemes, online shopping frauds, lottery and giveaway scams, and job offer frauds, often luring victims with unrealistic promises or fabricated urgency. Charity scams and social engineering attacks leverage public sympathy and social trust to elicit donations or personal information. Additionally, clickbait links, identity theft, Ponzi and pyramid schemes, and fabricated reviews or endorsements further contribute to the erosion of digital trust. These evolving threats underscore the need for enhanced user awareness, stronger platform-level safeguards, and robust policy interventions to mitigate the risks associated with social media–enabled fraud.

Digital banking Frauds

These frauds have become progressively escalating and prevalent with the widespread adoption of online and mobile commercial services. A significant portion of these frauds stem from the misuse of digital payment applications, where unsuspecting users are tricked into transferring money through fake customer service calls, phishing links, or unauthorized UPI requests. Another critical vulnerability lies in the hacking of bank accounts due to weak or reused passwords, which enables cybercriminals to gain unauthorized access to sensitive financial data. The practice of using the same password across multiple accounts further amplifies the risk, allowing attackers to compromise several services once one account is breached. These issues highlight the pressing need for stronger user authentication practices, better cybersecurity awareness among consumers, and enhanced regulatory oversight to secure digital banking ecosystems.

Cybersecurity threats

They increasingly target personal devices through both mobile applications and personal computers, making individual users highly vulnerable. Mobile application-based attacks often involve the installation of seemingly legitimate apps that are secretly embedded with malicious code. These infected apps can exfiltrate personal data, track user activity, or grant remote control access to attackers. Similarly, virus attacks on personal computers typically occur through the use of external storage devices, downloading files from untrusted websites, or installing malicious software disguised as legitimate tools. These vectors serve as entry points for malware, ransomware, or spyware, which can lead to security breach, malicious activities, corruption, or monetary loss. The increasing sophistication of such attacks underscores the importance of digital hygiene, including cautious app installation, secure browsing practices, and the use of updated antivirus software

To conclude, the growing digital footprint of individuals has made the protection of personal information more critical than ever. Section 2 explored various risks associated with personal data sharing, drawing from the insights of Agarwal (2023), who emphasized the interplay between legal frameworks, technological safeguards, and ethical responsibilities in the digital age. Furthermore, the classification of cybercrimes as outlined by the Government of India (cybercrime.gov.in) provided a structured understanding of prevalent threats, including identity theft, phishing, social media frauds, digital banking frauds, and mobile-based attacks. This discussion highlights the urgent need for enhanced digital literacy, stronger regulatory mechanisms, and cross-sector collaboration to guarantee and specify a safer and more secure online environment.

3.3 Internet Privacy in India

This section focuses on Internet Privacy in India and discusses the Data protection laws and the challenges in enhancing data protection awareness among users to empower them in making informed digital decisions.

Data Protection Policies

Data protection in India is governed by specific policies intended to secure personal information. Here, let us understand the evolution of privacy laws that has been shaped over many years by several developments and judicial decisions, enforcing the growing significance of protecting personal data.

Evolution of Indian Privacy Laws

The Information Technology Act (ITA)

The Information Technology Act (ITA) 2000 is an Act to provide official acknowledgment for transactions carried out by means of electronic data interchange and other modes of digital communication, commonly referred to as "electronic commerce", which involve the use of other options to paper-based methods of communication and storage of information.

The Act which was India's first legislation on the act of privacy and online safety marked a crucial step towards governing Information Technology in India, e- commerce and combatting cybercrime challenges and also specifies the penalties to those committing them, thereby aiming to protect the data security and privacy in the digital world.

The Act which had 94 sections included features which legally validated all contracts executed electronically, and a regulatory framework for e signatures using cryptosystem was also added. Electronic evidence was certified. Arrangements to set up a Cyber Regulations Advisory Committee to direct and instruct the Controller and the central government also existed as per the Act. The act has been amended over time to strengthen data protection measures and address emerging cyber threats.

2008 Amendment to ITA: The ITA 2000[9] was amended in 2008 to address emerging cyber threats more comprehensively. This amendment introduced sections dealing with identity theft, cyber terrorism, and the liability of intermediaries. It also emphasized the protection of sensitive personal data.

Key aspects of the ITA 2000 include:

1. **Legal Recognition of Electronic Documents**: The Act grants legal validity to electronic documents, making them an alternative to hard copy documents in terms of legal standing.
2. **Digital Signatures**: It recognizes the use of electronic or e signatures providing a secure and authentic means of signing electronic documents.
3. **Cybercrimes**: The ITA 2000 outlines specific offenses such as hacking, identity theft, cyberstalking, trespassing which are unauthorized access to computer systems. It prescribes penalties and punishments for these offenses.
4. **Intermediaries' Liability**: The Act defines the role and responsibilities like mediation, brokering, liaison, negotiation of intermediaries of internet service providers, in ensuring that their platforms are not used for illegal activities. It provides certain exemptions from liability if they follow due diligence.
5. **Data Protection**: Provisions for data protection are included, emphasizing the need for upholding sensitive information and protecting the confidentiality and integrity of personal information.
6. **Establishment of Authorities**: The Act establishes the Cyber Regulations Advisory Committee and the Cyber Appellate Tribunal to address disputes and provide guidance on cyber regulations.

Overall, the ITA 2000[9] is a significant and crucial legislation in India's efforts to regulate the digital space, enhance cybersecurity, and protect the interests of individuals and businesses engaging in electronic transactions.

India's Data Protection Law: A Timeline

In 2011, the Planning Commission set up an Expert Committee on Privacy, chaired by Justice A.P. Shah, to study international privacy laws, recognising data braches , and draft suggestions for a Privacy Bill.

The committee's 2012 report recommended creating a comprehensive privacy protection law based on five key features:

1. Technological Neutrality and Interoperability with International Standards
2. Multi-dimensional Privacy
3. Horizontal Applicability
4. Conformity with Privacy Principles
5. Co-regulatory Enforcement Regime

The report proposed nine national privacy principles as the foundation for privacy legislation:

1. Notice: Inform individuals during data compilation like data breaches.
2. Choice and Consent: Acquaint persons to make informed decisions about providing personal information and withdrawing consent.
3. Collection Limitation: Collect only the necessary information for the intended purpose.
4. Purpose Limitation: Ensure data collected is relevant to its purpose.
5. Access and Correction: Allow individuals to rectify and approach their personal information.
6. Disclosure of Information: Share personal information with third parties only with advance warning and informed concurrence.
7. Security: Implement appropriate measures and suitable precautions to protect personal information.
8. Openness: Take necessary steps proportional to the data's scale, scope, and sensitivity.
9. Accountability: Securing compliance and adhere to security measures.

In 2017, the Supreme Court of India, in the landmark case Justice K.S. Puttaswamy (Retd.) vs. Union of India, recognized the right to privacy as a fundamental right under Article 21 of the Indian

Constitution[5]. The court held that any infringement on privacy must fulfil and satisfy the legality (a legislative mandate), a legitimate state aim, and proportionality.

Following this, the Ministry of Electronics and Information Technology (MeitY) established a committee chaired by Justice B.N. Srikrishna to address data protection issues and draft a Data Protection Bill. The committee's 2018 report, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians," and the draft Personal Data Protection Bill 2018 were released for public feedback. A draft bill was prepared and feedback from public was extensively sought for nearly two months.[11]

These documents, along with stakeholder input, informed the Personal Data Protection Bill 2019, introduced in Parliament in December 2019 and is consulted to a Joint Parliamentary Committee (JPC)[12]. The JPC conducted extensive consultations and proposed 81 amendments, expanding the scope to include non-personal data. In August 2022, the Bill was withdrawn from Parliament due to significant amendments and bottlenecks and hurdles from Indian start-ups and the tech industry. In November 2022, MeitY released a draft of the Digital Personal Data Protection Bill 2022 for public consultation[13].

In August 2023, the Digital Personal Data Protection Bill 2023 was established in the Parliament. Fundamental differences from the draft included provisions for personal data processing outside India based on a country's disallowed list, broadened a comprehensive exemption for government data processing, and a reworked appeals process designating the Telecom Disputes Settlement and Appellate Tribunal as the appellate authority. The Bill was approved and adopted by both houses, received the president's assent, and became the Digital Personal Data Protection Act 2023[14].

As on January 2025[15], Indian data privacy rules are articulated placing their citizens at great importance. They insist on data fiduciaries required to provide genuine, accessible information about how user's personal information is processed, and only after getting informed consent from them. Indian citizens are empowered with rights which entail them to demand data erasure, and appoint digital nominees. Grievance redressal system enhances trust on the digital platforms.

In conclusion, Section 3 has traced the evolution of India's data protection landscape constituting the foundational Information Technology Act of 2000 to the enactment of the Digital Personal Data Protection Act, 2023. This legal path emphasises India's growing recognition of privacy as a fundamental right and the pressing necessity to regulate the electronics processing of personal information. While these legislative milestones mark significant progress, several critical challenges remain in translating these frameworks into effective, user-centric protections.

A major concern is the low level of digital literacy, particularly in rural and underserved populations, which limits users' ability to understand privacy implications and exercise their rights. Informed consent mechanisms are often overly complex, deterring meaningful engagement. Moreover, enforcement of data protection regulations remains inconsistent due to a lack of resources, limited training among enforcement personnel, and fragmented implementation across sectors. Awareness campaigns are sporadic and fail to reach broader audiences, while unregulated digital services continue to collect and misuse data with minimal oversight. The rapid pace of technological advancement, including AI and IoT, frequently outstrips regulatory developments, creating governance gaps. Additionally, concerns around government surveillance and data access challenge the trustworthiness of the system.

Addressing these challenges will require a multi-pronged approach involving robust enforcement, inclusive education, transparent governance, and sustained collaboration between policymakers, industry stakeholders, and community organizations. India's data protection framework not only exists in law but functions meaningfully in practice too.

CONCLUSION

The information, awareness and level of understanding or usage of data privacy laws among Indian customers is low. People may not grasp the diverse threats until each one goes through the menace, unlike the urban computer literate technologically competent and proficient. A distinct civic segment particularly the rural and semi-urban areas do not have recognition and realization of Personal Data Protection Bill. There is a paucity and deficit of detailed knowledge of rights and protection. The best part of the climax pinnacle is the need for ideal functioning democracy and a just society. Nonetheless the urban citizens still lack a substantial knowledge regarding the GDPR laws and rights to understand remedial process and prevent the disaster.

Customer awareness is the key element and major driving force in educating digital literacy[9]. Legal slangs lead to ignorance and uncertainty and stopping them from taking reasonable well informed decisions about their personal data. To spread this information more aggressive initiatives and strategic operations can be started by both government and private sector organisations.

Compliances with privacy seems to be a crucial step in this digital decade where strict regulations have become worrisome to customers[16]. However, it is important for institutions and government organisations to ensure all citizens to be well

informed, spread awareness, communicate privacy rights, user friendly, equipping them with tools, access policy rules and trained individuals about their rights and responsibilities under privacy laws.

There is lack of inactivity and passive involvement when accepting policy agreements at the end of an application. An energetic and enterprising configuration is required to instil and foster trust in customers for a secured digital process. Empowering consumers with the tools and knowledge to protect their digital privacy is top priority to build committed, enduring relationships in business.

Making headways there is an absolute necessary for the entire ecosystem to enthusiastically involve in developing and implementing digital privacy practices which will lead to a safe, honest, open and clear habitat.

Questions for future study in data privacy

(1) How can we monitor, transform, restyle the mounting intense duress from consumers to have a transparent privacy statement?
(2) What extra safety and preventive measures could be taken currently and what changes can be implemented tomorrow?
(3) What efforts can be initiated to be the trailblazer?.

REFERENCES

1. Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers*, *16*(2), 2577-2587.
2. Ezeocha, C. M. (2024). Digitalized Banking in a Globalized World: A Review of Nigeria's Digital Banking Transformation. *African Journal of Management and Business Research*, *16*(1), 53-68.
3. Drachsler, H., & Greller, W. (2016, April). Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In *Proceedings of the sixth international conference on learning analytics & knowledge* (pp. 89-98).
4. Rakha, N. A. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, *1*(1).
5. Wewege, Luigi & Lee, Jeo & Thomsett, Michael. (2020). Disruptions and Digital Banking Trends. 1792-6599.
6. Ezeocha, C. M. (2024). Digitalized Banking in a Globalized World: A Review of Nigeria's Digital Banking Transformation. *African Journal of Management and Business Research*, *16*(1), 53-68.
7. Chaudhry, Umair B., and Aysha KM Hydros. "Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm." *IET blockchain* 3, no. 2 (2023): 98-115.
1. 8.Government of India. (2000). The Information Technology Act, 2000. https://www.indiacode.nic.in/handle/123456789/1999
2. 9.Government of India. The Information Technology Act, 2000. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=
10. Agarwal, A. (2024, August 20). Right to privacy in digital age: Challenges and solutions. SSRN. https://ssrn.com/abstract=4955726
11. Ministry of Electronics and Information Technology. (2024, February). Public given 10 more days to give views on Draft Personal Data Protection Bill. https://www.meity.gov.in/static/uploads/2024/02/d12dbee367bcea98875462d1cba63689.pdf
12. PRS Legislative Research. (2019). The Personal Data Protection Bill, 2019. https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf
13. Ministry of Electronics and Information Technology. (2022). The Digital Personal Data Protection Bill, 2022. https://www.meity.gov.in/static/uploads/2024/02/The-Digital-Personal-Data-Potection-Bill-2022_0.pdf
14. Ministry of Electronics and Information Technology. (2023). The Digital Personal Data Protection Act, 2023, https://www.meity.gov.in/static/uploads/2024/02/Digital-Personal-Data-Protection-Act-2023-1.pdf
3. 15.Press Information Bureau., Draft Digital Personal Data Protection Rules. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2090271
15. Comptroller and Auditor General of India. (2024, October 8). Data protection and data privacy. https://cag.gov.in/uploads/icisa_virtual_publishing/Journal-with-cover-DG-message-08-10-2024-06704c77f434894-25842653.pdf