NATIONAL LAW INSTITUTE UNIVERSITY BHOPAL

Master of Cyber Law and Information Security

BATCH 2024-26

WEB APPLICATION SECURITY AND LAW

Project Assignment On

"ANALYTICAL STUDY OF WEB APPLICATION PRIVACY POLICIES: ASSESSING COMPLIANCE WITH LEGAL AND REGULATORY FRAMEWORKS."

Under the Supervision of

Dr. AMITESH SINGH RAJPUT

Assistant professor

Computer science

Submitted By

MEENAKSHI PUNDHIR
2024MCLIS27

II semester

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere gratitude to everyone who has supported me throughout the course of my project on *"Analytical Study of Web Application Privacy Policies: Assessing Compliance with Legal and Regulatory Frameworks."*

First and foremost, I am profoundly grateful to *Dr. S. Suryaprakash,* our Vice Chancellor, whose unwavering encouragement and support have been invaluable in helping me overcome challenges and pursue excellence in my research.

I also extend my heartfelt appreciation to *Mr. Vivek Bakshi,* our Registrar, for his guidance and constant willingness to assist, ensuring that I had the necessary resources and confidence to progress smoothly.

A special note of thanks goes to my professor, *Dr. Amitesh Singh Rajput,* whose mentorship has been instrumental in refining my research. His insightful feedback and valuable suggestions have significantly enhanced the quality of my work.

Lastly, I would like to acknowledge the Library staff of National Law Institute University, Bhopal, for their invaluable assistance in providing access to crucial resources that played a pivotal role in the successful completion of my project.

I deeply appreciate the support and encouragement I have received from everyone involved, and I am truly grateful for their time and effort in helping me achieve this milestone.

Meenakshi Pundhir

Roll No. 2024MCLIS27

II Semester

Contents

ABSTRACT

In today's digital landscape, web applications have become an integral part of everyday life, handling vast amounts of personal data. Privacy policies act as a critical safeguard, outlining how user information is collected, processed, and protected. This study takes a deep dive into the structure and effectiveness of privacy policies in web applications, analysing their role in ensuring compliance with regulations like GDPR, CCPA, and HIPAA. It examines key aspects such as data collection practices, user consent mechanisms, third-party data sharing, and security measures. Additionally, the study explores how emerging technologies—including APIs, cloud services, and IoT devices—introduce new challenges for privacy protection. By assessing industry practices and legal frameworks, this research highlights gaps, inconsistencies, and potential improvements, advocating for privacy policies that are not just legally sound but also transparent and user-friendly.

Keywords: Privacy policies, web applications, data protection, GDPR, user consent, API security, compliance, digital privacy, regulatory frameworks.

CHAPTER 1: INTRODUCTION

A privacy policy is an essential document that informs users about how a website or app gathers, processes, and uses their personal information. It outlines users' rights regarding their data and provides instructions on how to exercise those rights. The content of a privacy policy varies based on the applicable data protection laws but typically includes the types of data collected, methods of collection, reasons for processing (legal basis), and whether the data is shared or sold to third parties. Factors such as the business's location, customer base, data volume, and revenue determine the legal requirement for a privacy policy. It differs from terms and conditions, which set rules for using the service, and disclaimers, which limit legal liability. Any business operating online, regardless of its size, should publish a comprehensive privacy policy to comply with regulations and build user trust.

The specifics of privacy policies are governed by various global data protection laws. Regulations like the *GDPR (EU), UK GDPR, CCPA (California), PIPEDA (Canada), and PoPIA (South Africa)* impose different requirements regarding transparency, user rights, and data protection. For example, *GDPR* mandates businesses to disclose data collection methods, storage durations, international transfers, and users' rights to request data corrections or deletions. Similarly, *CalOPPA* requires businesses to outline their data collection practices, how users can opt out, and whether they honour *Do Not Track (DNT)* requests. Adhering to these regulations helps businesses avoid legal penalties and build a trustworthy reputation.

Privacy policies play a key role in earning customer trust, as many users prefer brands that handle personal data responsibly. Research shows that consumers are more likely to abandon purchases or services if they feel their information is mishandled. Additionally, third-party services like WordPress, Google Analytics, and Shopify require businesses to publish privacy policies to use their platforms. By creating a clear and legally compliant privacy policy, businesses can demonstrate their commitment to data protection, strengthen customer confidence, and avoid regulatory fines.

Beyond legal compliance, a well-structured privacy policy also serves as a competitive advantage. In an era where data breaches and cyber threats are increasing, businesses that prioritize transparency and data security can differentiate themselves from competitors. Clearly communicating privacy practices reassures customers and fosters long-term relationships. Moreover, as consumer awareness of digital rights grows, companies with robust privacy policies are more likely to attract and retain users who value data protection. Thus, investing in a strong privacy policy is not just a legal necessity but also a strategic move to enhance brand credibility and customer loyalty.

1.1 REVIEW OF LITERATURE

- ***Nishchay Nagarwal, "Privacy Policy and Data Protection Laws in India" (2020):*** This article explores the growing importance of privacy policies in India's digital economy. With businesses collecting vast amounts of user data, privacy policies act as legal agreements that outline data collection, usage, and protection practices. While the IT Rules, 2011, mandate intermediaries to publish privacy policies, the absence of a dedicated data protection law raises concerns about enforcement and user rights. The study highlights the need for stronger privacy frameworks to ensure transparency, compliance, and consumer trust.
- ***Wiliam Blesch, "What Does a Privacy Policy Need to Include" (2025):*** This article highlights the importance of privacy policies in meeting legal requirements like GDPR and CCPA. It explains that businesses must clearly outline how they collect, use, and share user data while informing users of their rights. Privacy policies should also be regularly updated and easy to understand to maintain transparency and compliance. Failing to do so can lead to legal penalties and a loss of customer trust.
- ***Abraham Mhaidli and others, "Researchers' Experiences in Analysing Privacy Policies: Challenges and Opportunities" (2023):*** This article explores the challenges researchers face when studying privacy policies and how technology is helping to address them. With the rise of NLP and machine learning, efforts are being made to analyse policies for clarity, compliance, and ease of understanding. However, issues like complex legal language, inconsistent formats, and difficulty in retrieving policies make research challenging. The study highlights the need for better tools, standardized approaches, and collaboration across different fields to improve transparency and protect user data.
- ***Karl van der Schyff and others, "Privacy policy analysis: A scoping review and research agenda" (2024):*** This article explores the challenges of understanding privacy policies, which are often complex and difficult to navigate. By reviewing 97 studies, it examines different analysis methods, including machine learning, natural language processing, and manual review. It highlights key issues like vague language and the absence of standardized frameworks, emphasizing the need for clearer, more user-friendly policies and better evaluation methods to improve transparency and compliance.

1.2 STATEMENT OF PROBLEM

Privacy policies in web applications often lack clarity in outlining user rights, data-sharing practices, and consent mechanisms. Many are overly complex, vague, or fail to provide transparency, making it challenging for users to grasp how their data is collected, used, or shared with third parties.

1.3 HYPOTHESIS

By analysing web application privacy policies, this study can uncover gaps in legal compliance, data collection transparency, user consent practices, and third-party data sharing. It helps identify inconsistencies that may lead to non-compliance or compromise user rights. Addressing these shortcomings can lead to more transparent, legally robust, and user-friendly privacy policies.

1.4 RESEARCH QUESTIONS

1. What are the core principles that form the foundation of effective privacy policies in web applications, and how do they safeguard user data?
2. How do existing legal and regulatory frameworks influence the structure and enforcement of privacy policies in web applications?
3. What patterns, gaps, and compliance issues emerge from an analytical study of privacy policies across 20 web applications?
4. What improvements or strategic measures can be implemented to enhance compliance, ensure transparency, and strengthen user trust in web application privacy policies?

1.5 RESEARCH OBJECTIVES

1. To identify and evaluate the fundamental tenets of privacy policies in web applications, focusing on key aspects such as user rights, data collection practices, consent mechanisms, third-party data sharing, and security measures.
2. To conduct an analytical study of privacy policies from 20 web applications, assessing their compliance with legal and regulatory frameworks, such as GDPR, CCPA, and other global data protection standards.
3. To examine the gaps and inconsistencies in the privacy policies of web applications, highlighting areas where they fall short in transparency, user control, and adherence to legal obligations.
4. To propose recommendations for enhancing privacy policies in web applications, ensuring they align with evolving regulatory requirements, address existing shortcomings, and provide users with greater control over their personal data.

1.6 SCOPE AND LIMITATION

This study analyses privacy policies of 20 web applications to assess their compliance with GDPR, CCPA, DPDPA, and HIPAA. It focuses on key aspects like user rights, consent, data retention, third-party sharing, and security measures. The scope is limited to publicly available privacy policies, excluding internal compliance mechanisms and jurisdictional variations beyond these regulations.

1.7 RESEARCH METHODOLOGY

The researcher has chosen the doctrinal method of research to investigate the topic of "Analytical Study of Web Application Privacy Policies: Assessing Compliance with Legal and Regulatory Frameworks."

CHAPTER 2: ANALYSIS AND DISCUSSION

A **privacy policy**[1] is a crucial document that explains how an organization collects, stores, and protects user data. It serves as a bridge of trust between businesses and users while ensuring compliance with data protection laws like GDPR[2], CCPA[3], and HIPAA[4]. A well-crafted privacy policy clearly outlines what data is collected, why it is needed, who has access to it, and how users can control their personal information. If a company lacks a transparent privacy policy, it risks legal trouble and losing customer trust.

Meanwhile, **web application security** is all about keeping online platforms safe from cyber threats like hacking, data breaches, and malware attacks. Common vulnerabilities—such as SQL injection, cross-site scripting (XSS), and denial-of-service (DDoS) attacks—can expose sensitive information, causing financial losses and reputational damage. To prevent such risks, organizations must prioritize security measures like encryption, strong authentication, regular security audits, and secure coding practices.

Privacy policies and web security go hand in hand—while the policy informs users about how their data is handled, security measures ensure that it stays protected. To build a truly secure digital environment, companies should implement industry standards like ISO 27001 and SOC 2, ensuring compliance and reinforcing user confidence. Techniques like data minimization and anonymization further reduce risks by limiting the amount of sensitive information stored.

As technology evolves, so do the risks to privacy and security. The rise of AI, cloud computing, and IoT devices has introduced new challenges that businesses must actively address. Regular security updates, compliance with global regulations, and continuous user education are essential to staying ahead of emerging threats. A strong commitment to both legal and security standards not only safeguards data but also strengthens a company's credibility and long-term success.

Beyond technical safeguards, cultivating a strong culture of privacy and security awareness is essential. Organizations should regularly train employees on cybersecurity best practices, conduct

[1] Ned Thornton, 'Privacy Policies: What They Are and Why They Matter' (*PrivacyEnd*, 30 August 2023) <https://www.privacyend.com/what-are-privacy-policies/> accessed 9 March 2025.
[2] 'General Data Protection Regulation (GDPR) – Legal Text' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/> accessed 9 March 2025.
[3] 'California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General' <https://www.oag.ca.gov/privacy/ccpa> accessed 9 March 2025.
[4] CDC, 'Health Insurance Portability and Accountability Act of 1996 (HIPAA)' (*Public Health Law*, 10 September 2024) <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html> accessed 9 March 2025.

phishing awareness exercises, and educate users on safe digital behaviors. Promoting transparency in data handling and embedding privacy-by-design principles from the start of development can further strengthen security. By combining robust security measures with ethical data management, businesses can build a trustworthy digital environment that protects user information while ensuring compliance with regulations.[5]

2.1 LEGAL AND REGULATORY FRAMEWORKS FOR PRIVACY POLICIES.

Privacy policies are shaped by various legal frameworks worldwide, ensuring that organizations handle personal data responsibly. These regulations set guidelines on data collection, processing, and user rights, making compliance essential for businesses to build trust and avoid penalties.

2.1.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), enforced by the European Union since 2018, is one of the most stringent privacy laws globally. It applies to any organization handling the personal data of EU residents, regardless of where the business is based. At its core, GDPR is built on principles such as transparency, fairness, and accountability. Companies must collect only the necessary data for a specific purpose, ensure its accuracy, store it securely, and not retain it longer than needed. The regulation also enforces the idea of "privacy by design," meaning businesses should integrate data protection measures from the outset rather than as an afterthought.

GDPR grants individuals significant control over their personal information. People have the right to access their data, correct inaccuracies, and even request its deletion under certain conditions (the "right to be forgotten"). They can also restrict how their data is processed, transfer it between services (data portability), and object to its use for purposes like marketing. For businesses, compliance involves conducting Data Protection Impact Assessments (DPIAs)[6] when handling sensitive data, appointing Data Protection Officers (DPOs) in specific cases, and promptly notifying authorities and users of any data breaches—typically within 72 hours. These measures aim to create a culture of data protection and accountability.[7]

---

[5] Nischay Nagarwal, 'Privacy Policy and Data Protection Laws in India' (*LegalWiz.in*, 3 July 2020) <https://www.legalwiz.in/blog/privacy-policy-and-data-protection-laws-in-india> accessed 6 March 2025.

[6] 'Data Protection Impact Assessment (DPIA)' (*GDPR.eu*, 9 August 2018) <https://gdpr.eu/data-protection-impact-assessment-template/> accessed 9 March 2025.

[7] 'General Data Protection Regulation (GDPR) – Legal Text' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/> accessed 9 March 2025.

2.1.2 California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

The California Consumer Privacy Act (CCPA), which took effect in 2020 and was later strengthened by the California Privacy Rights Act (CPRA) in 2023, gives California residents greater control over their personal data. These laws focus on transparency and user choice, ensuring businesses clearly disclose how they collect, share, and use consumer data.

Under these laws, consumers have the right to know what data is being collected and how it is shared, the right to delete their personal information, and the right to opt out of the sale of their data. The CPRA further expands these protections by introducing the right to correct inaccurate data and the ability to limit the use of sensitive personal information, such as financial details, health records, or location data. To comply, businesses must provide clear privacy notices and include a "Do Not Sell or Share My Personal Information" option on their websites. Additionally, companies handling large volumes of personal data must conduct risk assessments and cybersecurity audits to ensure data protection. These regulations mark a shift towards stronger consumer privacy rights in the U.S. and set a precedent for future privacy laws.[8]

2.1.3 Digital Personal Data Protection Act (India)

India's Personal Data Protection Bill (PDPB), now formalized as the Digital Personal Data Protection Act (DPDPA), 2023, is a significant step toward safeguarding personal data. It applies to all entities handling Indian users' data, including foreign organizations. The law emphasizes consent-driven data processing, meaning businesses must obtain explicit permission before collecting or using personal information. It also gives individuals key rights, such as accessing their data, requesting corrections, and even asking for its deletion in certain cases.

Companies handling large amounts of sensitive data are categorized as Significant Data Fiduciaries (SDFs) and are subject to stricter compliance requirements, including privacy-by-design policies, regular audits, and impact assessments. One notable feature of the DPDPA is its data localization requirement, which mandates that certain categories of personal data be stored within India to enhance security. A Data Protection Board has also been established to oversee compliance and impose penalties for violations. While this law strengthens privacy rights, businesses may face higher

[8] 'California Consumer Privacy Act (CCPA)' (*State of California - Department of Justice - Office of the Attorney General*, 15 October 2018) <https://oag.ca.gov/privacy/ccpa> accessed 9 March 2025.

compliance costs as they adapt to these new regulations. In the long run, however, it is expected to improve digital trust and security for Indian consumers.[9]

2.1.4 Other Global Privacy Regulations

Apart from GDPR, CCPA, and India's DPDPA, various other privacy laws regulate specific industries and regions. The Health Insurance Portability and Accountability Act (HIPAA) in the United States, for example, focuses on protecting patient health information. Healthcare providers, insurers, and associated businesses must follow strict rules to ensure Protected Health Information (PHI) remains confidential. Patients must give consent before their medical data can be shared, and companies are required to implement strong security safeguards to prevent breaches. Non-compliance can lead to hefty fines and legal consequences.

For children's online privacy, the Children's Online Privacy Protection Act (COPPA)[10] is a crucial U.S. law that governs how websites and apps collect data from users under 13 years old. Companies must get verifiable parental consent before gathering any personal details from children. COPPA also enforces strict data deletion policies and requires businesses to clearly explain their data practices in a way that parents can understand.

Other noteworthy privacy laws include Brazil's General Data Protection Law (LGPD)[11], which closely mirrors GDPR, and Australia's Privacy Act, which regulates how businesses collect and use consumer data. China's Personal Information Protection Law (PIPL)[12] imposes some of the world's strictest data transfer restrictions, requiring companies to get consent before processing personal data and enforcing strict penalties for violations. These global regulations highlight the growing emphasis on data privacy, pushing businesses to adopt stronger security and compliance measures.[13]

2.2 FUNDAMENTAL TENETS OF A PRIVACY POLICY.

A privacy policy is more than just a legal requirement—it's a bridge of trust between a web application and its users. In an era where personal data is constantly being collected, stored, and analyed, users deserve clarity on how their information is handled. A well-structured privacy policy ensures transparency, complies with regulations like the General Data Protection Regulation (GDPR)

[9] 'Digital Personal Data Protection Act 2022/23' <https://www.dpdpa.in/> accessed 9 March 2025.
[10] 'Http://Www.Ftc.Gov/Ogc/Coppa1.Htm'.
[11] 'LGPD Brazil - General Personal Data Protection Act' <https://lgpd-brazil.info/> accessed 9 March 2025.
[12] 'The PRC Personal Information Protection Law (Final): A Full Translation' (*China Briefing News*, 24 August 2021) <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/> accessed 9 March 2025.
[13] Abraham Mhaidli and others, 'Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities' (2023) 2023 Proceedings on Privacy Enhancing Technologies 287.

and California Consumer Privacy Act (CCPA), and reassures users that their data is being treated with care. The goal is to present this information in a way that is clear, concise, and easy to understand, avoiding unnecessary legal jargon.

2.2.1 Data Controller and Contact Information

The first step in building trust is letting users know exactly who is responsible for handling their data. The privacy policy should clearly state the name of the organization, its address, and relevant contact details. If a Data Protection Officer (DPO) has been appointed—something required under GDPR in certain cases—their contact information should also be provided. This allows users to reach out if they have concerns about how their data is being used or if they need assistance exercising their rights.

2.2.2 Types of Data Collected

Every interaction with a web application involves some form of data collection. This could be as simple as a name and email address when signing up or as complex as tracking browsing behavior through cookies. The policy should clearly define the types of data collected, breaking them down into personal data (such as names, email addresses, and payment details) and non-personal data (such as IP addresses, device information, and browsing history). If sensitive data like biometric or health-related information is collected, that should be explicitly mentioned, along with details about how it's safeguarded.

2.2.3 Purpose of Data Collection

Users should never be left guessing why their data is being collected. Whether it's for creating an account, processing transactions, improving services, or sending personalized recommendations, every reason should be stated upfront. If data is being used for automated decision-making—like AI-driven recommendations or credit scoring—the policy should explain what this means and how it affects users. Transparency in this area reassures users that their data isn't being misused.

2.2.4 Legal Basis for Processing Data

Under regulations like GDPR, organizations must have a valid reason for processing personal data. These legal grounds typically fall into a few categories:

- User Consent – When users actively agree to things like marketing emails or cookie tracking.
- Contractual Necessity – When data is needed to fulfill a service, such as processing an order.
- Legal Obligations – When laws require data collection, such as for tax or fraud prevention.

- Legitimate Interests – When data is used for security, fraud detection, or business analytics—provided it doesn't violate user rights.

If legitimate interest is the justification, the policy should explain why and how the organization ensures user privacy remains a priority.[14]

2.2.5 Data Retention Policy

Users have the right to know how long their data is kept and when it will be deleted. The privacy policy should outline retention periods—whether data is kept for a set number of years, deleted upon account closure, or anonymized for research purposes. GDPR also grants users the right to erasure, meaning they can request their data be permanently deleted. The policy should explain how users can make such requests and what exceptions might apply (for example, if legal obligations require retaining certain information).

2.2.6 Data Sharing and Third-Party Disclosures

Most web applications rely on third-party services for payments, analytics, or cloud storage. The privacy policy should be upfront about who these third parties are and whether any data is shared with them. If user data is transferred across borders—such as from the EU to the U.S.—the policy should explain what safeguards are in place, like *Standard Contractual Clauses (SCCs)* or *Binding Corporate Rules (BCRs).* By being transparent about these practices, organizations can help users feel more in control of their information.[15]

2.2.7 User Rights and Controls

People are increasingly aware of their data rights, and a privacy policy should empower them to exercise those rights. Under GDPR, users have the right to:

- Access their data and see what information is being stored.
- Correct inaccuracies if their details are outdated or incorrect.
- Request deletion of their data (the "right to be forgotten").
- Restrict how their data is used if they're uncomfortable with certain processing activities.
- Move their data to another service if they want to switch providers.

[14] Karl van der Schyff, Suzanne Prior and Karen Renaud, 'Privacy Policy Analysis: A Scoping Review and Research Agenda' (2024) 146 Computers & Security 104065.
[15] Thornton (n 1).

- Object to marketing or automated decision-making processes.

Similarly, under CCPA, users can request details on how their data has been used in the past 12 months and opt out of having their personal information sold. The privacy policy should provide clear instructions on how to make these requests—whether through a dedicated portal, email, or customer service contact.

2.2.8 Cookies and Tracking Technologies

Most websites use cookies and tracking tools to improve user experience, analyze performance, or serve targeted ads. The privacy policy should explain:

- What types of cookies are used (essential cookies for functionality, analytics cookies for tracking, and marketing cookies for advertising).
- Whether third-party tracking tools are involved, such as Google Analytics or Facebook Pixel.
- How users can manage cookie preferences, including opting out where required by laws like the e-Privacy Directive in Europe.

Since cookies can impact user privacy, offering a clear opt-in mechanism for non-essential cookies ensures compliance and builds trust.

2.2.9 Children's Privacy

If a web application is used by children, additional regulations apply. In the U.S., COPPA (Children's Online Privacy Protection Act) sets strict rules on collecting data from children under 13. Similarly, the GDPR-K provision requires parental consent for processing data of children under 16 in some European countries. The privacy policy should clearly state:

- Whether the service is meant for children.
- If parental consent is required.
- How children's data is collected, used, and deleted.
- If the platform isn't designed for children, the policy should state this explicitly and outline measures taken to prevent unintentional data collection.

2.2.10 Contact Information and Complaints

If users have concerns about their data, they should know exactly where to turn. The privacy policy should include a clear point of contact—whether an email address, privacy officer, or a dedicated support team. Additionally, it should mention users' rights to escalate complaints to a data protection

authority, such as the Information Commissioner's Office (ICO) in the UK or the relevant Data Protection Authority (DPA) in their country.[16]

2.3 PRIVACY POLICY ANALYSIS AND FINDINGS.

This study analysed the privacy policies of various web applications to evaluate their compliance with regulations like GDPR, CCPA, and PCI DSS. The process involved reviewing policies in detail, identifying key aspects such as cookie usage, data security, tracking methods, and user control options, and comparing them across different platforms. Applications that lacked clear cookie policies, opt-out choices, or strong security measures were marked as high-risk due to potential privacy concerns. The findings highlighted gaps in transparency and legal compliance, leading to recommendations for improving data protection, enhancing user privacy, and ensuring better regulatory adherence.

2.3.1 Key Compliance Parameters

The dataset evaluates web applications based on their adherence to legal and regulatory requirements, including:

- CCPA Compliance (Required/Not Required)
- PCI DSS Compliance (Yes/No)
- Data Security Measures (Yes/No)
- Tracking & Cookies Usage (Yes/No)
- Presence of Cookie Policies and Notices
- Opt-Out Clauses for Data Collection
- Minor Protection Measures

2.3.2 Major Compliance Issues

a) Lack of Clear Cookie Policies

- Several applications (Meesho, Flipkart, Groww, Turbo VPN) do not provide a dedicated cookie policy or notice.
- This violates transparency principles under GDPR and CCPA, which require informing users about tracking technologies.

[16] 'What Does a Privacy Policy Need to Include?' (*TermsFeed*, 16 February 2025) <https://www.termsfeed.com/blog/privacy-policy-needs-to-include/> accessed 6 March 2025.

- Users may not be aware of what data is being collected via cookies and how it is used for behavioural tracking, analytics, or third-party sharing.

b) Tracking & Cookies Usage Without Transparency

- All applications use cookies and tracking technologies but fail to consistently provide clear consent mechanisms.
- Regulations like GDPR and e-Privacy Directive mandate cookie consent pop-ups, but some platforms lack them entirely.
- Potential risks include unauthorized data collection, profiling without user consent, and non-compliance penalties.

c) CCPA Compliance Gaps

- Some applications comply with CCPA, but others claim compliance is not required (e.g., Meesho, Flipkart, Groww, Turbo VPN).
- However, CCPA still applies to apps handling data of California residents, meaning some may be non-compliant by failing to provide a proper opt-out mechanism.

d) Weak Opt-Out Mechanisms

- While Zomato, Truecaller, and Flipkart provide opt-out clauses, platforms like Meesho, Groww, and Turbo VPN lack this option.
- Without opt-out mechanisms, users cannot prevent data collection, making these applications less privacy-friendly.

e) Data Security and Minor Protection Issues

- Groww lacks explicit security measures, which is a critical concern for a financial platform.
- Flipkart and Groww do not have proper minor protection clauses, making them non-compliant with child data protection laws like COPPA and GDPR.

2.3.3. Implications of Missing Cookie Policies

- Legal Risks: GDPR and CCPA require websites to provide detailed cookie notices and allow users to opt out. Failure to comply can lead to fines and regulatory actions.
- User Mistrust: Without clear policies, users may not trust the platform's data practices, leading to reputational risks.

- Hidden Data Collection: Tracking without disclosure increases concerns about unauthorized profiling and third-party data sharing.

2.3.4. Recommendations to Improve Compliance

- Implement clear, dedicated cookie policies outlining the types of cookies used, their purpose, and how users can manage them.
- Ensure GDPR and CCPA compliance by providing opt-in mechanisms and consent banners.
- Enhance transparency by detailing cookie retention periods and third-party integrations.
- Regularly update privacy policies to reflect evolving data protection laws.

COMPARATIVE ANALYSIS OF PRIVACY POLICIES

Serial NO.	Web Application Name	Web Application Description	Website URL	Date of Last Policy Update	Data Collected (Y/N)	Types of Data Collected	Purpose of Data
1	ZOMATO	Zomato is an Indian food delivery and restaurant discovery platform offering online ordering, reviews, and dining-out services. It collects and processes user data, including location, order history, and preferences, to personalize recommendations, enhance services, and optimize delivery logistics. The platform also shares data with restaurant partners and third-party service providers while adhering to privacy regulations.	https://www.zomato.com/policies/privacy/	22-04-2020	YES	Account details, profile picture, third-party sign-in, preferences, settings, content, reviews, photos, reservations, search history, browsing activity, ads clicked, communications, surveys, promotions, transactions, payment data, public posts, user contributions, friend invitations, messaging logs, SMS data, usage stats, traffic logs, device info, IP address, OS details, browser type, stored files, metadata, location tracking, last URL, mobile IDs, analytics, advertising, app presence, online status, personalization.	Specified
2	Truecaller	Truecaller is a caller ID and spam-blocking app that identifies incoming calls, blocks unwanted numbers, and provides contact details from its global database. It also offers messaging, call recording, and payment services in some regions. The app crowdsources data from users to enhance its directory and spam detection capabilities.	https://www.truecaller.com/privacy-policy	04-10-2024	YES	User profile includes name, phone number, email, address, social media, and verification via SMS/missed call, with third-party data supplementation. Installation and use involve collecting IP address, location, device ID, SIM data, installed apps, usage stats, communication logs, browsing behavior, ads, and cookies. Third-party services access social media, payment platforms, user IDs, transactions, and ads, with privacy settings control. Contact information may include address book access (if outside App Store/Google Play), phone numbers, names, and email IDs, with filtering and opt-out options. User interaction features tagging, spam reports, surveys, identity verification, and third-party authentication.	Specified
3	MEESHO	Meesho is an Indian e-commerce platform that primarily facilitates social commerce, allowing small businesses and individual resellers to sell products through social media platforms like WhatsApp, Facebook, and Instagram. It operates as a marketplace connecting suppliers and buyers, handling logistics, payments, and customer service.	https://www.meesho.com/legal/privacy	10-04-2023	YES	Meesho collects and processes user data, including personally identifiable details like name, contact, Aadhaar, PAN, and financial information, along with user preferences, browsing behavior, search history, and transaction details. It tracks device and location data, social media integrations, and interactions such as reviews, chats, and promotions. The platform also uses cookies, mobile IDs, and analytics for personalization, targeted ads, security, fraud prevention, and regulatory compliance, ensuring seamless transactions and service optimization.	Specified

Purpose of Data Collection	What is the Purpose of Data Collection	Data Sharing (Y/N)	With Whom Data is Shared	Third Parties Involved	Data Retention Period	User Rights Mentioned (Y/N)	What Rights does Users Have	GDPR Compliance (if req
Specified	Process and respond to queries, understand users and their behavior, improve content and features, administer services and fix technical issues, send user-generated questions, show relevant ads, generate reports and study usage patterns, administer contests and sweepstakes, provide customer assistance, share account policies, fulfill contractual obligations and handle billing, update users on service changes, enable participation in interactive features, use information as described at the time of collection, use information for additional purposes with permission.	YES	Subsidiaries, affiliates, contractors, advertisers, business transfers, third-party marketers, disclosed purposes, user-specified purposes, service providers, legal compliance, law enforcement, fraud protection, social media, enforce terms, consent-based sharing, restaurant reservations, payment processors, stored payment data, analytics, tracking, tailored advertising, ad targeting, opt-out mechanisms.	YES	YES	YES	**Right to information** - including contact details to the DPO, the purposes for processing Personal Information and the rights of the individual. **Right to access the Personal Information** that are processed **Right to erasure** (**"Right to be forgotten"**) **Right to rectification** **Right to restriction of processing** **Right to data portability** of the Personal Information supplied to Zomato by the EU resident **Right to object**	COMPLIANT (Required)
Specified	***Service improvement***: caller ID, dialer, messaging, unidentified number identification, name/number search, social graph, profile views, push notifications, spam blocking, third-party integration, verified business call logs, analytics. ***Statistical data***: anonymized, aggregated, shared with third parties. ***Advertising & communication***: location-based ads, marketing, performance measurement, verification, service updates, newsletters, partner promotions, user response. ***Compliance & security***: legal adherence, fraud prevention, profile verification, troubleshooting, security, breach detection.	YES	vendors, service providers, partners, infrastructure providers, bug testers, analytics firms, ad measurement agencies, payment facilitators, potential collaborators, affiliated entities, business acquirers (merger, consolidation, asset purchase)	YES	YES	YES	Right to Access, Right to Be Informed, Right to Rectification, Right to Erasure, Right to Object, Right to Restriction, Right to Data Portability, Right to Object to Automated Decision-Making, and Right to Withdraw Consent.	COMPLIANT (Required)
Specified	Meesho utilizes collected data for order fulfillment, personalized recommendations, targeted advertising, fraud prevention, legal compliance, and communication via multiple channels. It assesses credit risks, manages billing, enforces contracts, administers promotions, and conducts user research to enhance services. Data is also used for marketing, analytics, and eligibility checks for financial products, ensuring a secure, customized, and seamless user experience.	YES	Meesho shares user data with affiliates, service providers, financial institutions, and third parties for business operations, payment processing, marketing, and research while ensuring confidentiality. Data may be disclosed during mergers, legal proceedings, or to enforce agreements. Credit analysis involves sharing with CICs for payment options. Legal compliance requires data sharing with authorities for investigations and fraud prevention. Social media interactions may collect and share data per their policies. Information is also shared for user safety, contract enforcement, and with consent, ensuring transparency and security in data	YES	YES	NO	User Rights are not specified	NO (Not Required)

GDPR Compliance (if required)	CCPA Compliance (if required)	PCI DSS Compliance	Data Security Measures Provided	Tracking and Cookie Used	Cookie Policy & Cookie Notice	Opt-Out Clause (Y/N)	Privacy Contact Info	Minor Protection Clause	Remarks	Remark Description
COMPLIANT (Required)	COMPLIANT (Required)	YES	YES	YES	PROVIDED	YES	PROVIDED	YES	SATISFACTORY	All important clauses are provided.
COMPLIANT (Required)	COMPLIANT (Required)	NO	YES	YES	PROVIDED	YES	PROVIDED	YES	SATISFACTORY	All important clauses are provided.
NO (Not Required)	NO (Not Required)	NO	YES	YES	NOT PROVIDED	NO	PROVIDED	YES	NEEDS IMPROVEMENT	ookie policy and Cookie notice is not provided.
NO (Not Required)	NO (Not Required)	NO	YES	YES	NOT PROVIDED	YES	PROVIDED	NO	NEEDS IMPROVEMENT	ookie policy and Cookie notice is not provided.

PRIVACY POLICY ANALYSIS REGISTER

Serial NO.	3
Web Application Name	MEESHO
Web Application Description	Meesho is an Indian e-commerce platform that primarily facilitates social commerce, allowing small businesses and individual resellers to sell products through social media platforms like WhatsApp, Facebook, and Instagram. It operates as a marketplace connecting suppliers and buyers, handling logistics, payments, and customer service.
Website URL	https://www.meesho.com/legal/privacy
Date of Last Policy Update	10-04-2023
Data Collected (Y/N)	YES
Types of Data Collected	Meesho collects and processes user data, including personally identifiable details like name, contact, Aadhaar, PAN, and financial information, along with user preferences, browsing behavior, search history, and transaction details. It tracks device and location data, social media integrations, and interactions such as reviews, chats, and promotions. The platform also uses cookies, mobile IDs, and analytics for personalization, targeted ads, security, fraud prevention, and regulatory compliance, ensuring seamless transactions and service optimization.
Purpose of Data Collection	Specified
What is the Purpose of Data Collection	Meesho utilizes collected data for order fulfillment, personalized recommendations, targeted advertising, fraud prevention, legal compliance, and communication via multiple channels. It assesses credit risks, manages billing, enforces contracts, administers promotions, and conducts user research to enhance services. Data is also used for marketing, analytics, and eligibility checks for financial products, ensuring a secure, customized, and seamless user experience.
Data Sharing (Y/N)	YES
With Whom Data is Shared	Meesho shares user data with affiliates, service providers, financial institutions, and third parties for business operations, payment processing, marketing, and research while ensuring confidentiality. Data may be disclosed during mergers, legal proceedings, or to enforce agreements. Credit analysis involves sharing with CICs for payment options. Legal compliance requires data sharing with authorities for investigations and fraud prevention. Social media interactions may collect and share data per their policies. Information is also shared for user safety, contract enforcement, and with consent, ensuring transparency

Third Parties Involved	YES
Data Retention Period	YES
User Rights Mentioned (Y/N)	YES
What Rights does Users Have	User Rights are not specified
GDPR Compliance (if required)	NO(Not Required)
CCPA Compliance (if required)	NO(Not Required)
PCI DSS Compliance	NO
Data Security Measures Provided	NO
Tracking and Cookie Used	NO
Cookie Policy & Cookie Notice	NOT PROVIDED
Opt-Out Clause (Y/N)	NO
Privacy Contact Info	PROVIDED
Minor Protection Clause	YES
Remarks	NEEDS IMPROVEMENT
Remark Description	Cookie policy and Cookie notice is not provided.

FIGURES: *Snippets from the analytical study of privacy policies in web applications.*

CHAPTER 3: CONCLUSION AND SUGGESTIONS.

As web applications become more complex and data-driven, privacy policies can no longer remain static, jargon-heavy documents that users skim through—or worse, ignore. Instead, they are evolving into interactive, user-friendly frameworks designed to offer real control over personal data. With advancements in AI, IoT, APIs, cloud computing, and evolving regulations, privacy policies must go beyond legal compliance and become practical tools that genuinely protect user information while maintaining transparency and trust.

Adaptive and Interactive Policies.

Most users don't read privacy policies because they are filled with legal terminology and tedious details. The future of privacy policies lies in clarity and adaptability. Imagine policies that adjust dynamically based on real-time privacy risks or automated summaries that explain key terms in simple language. AI-driven assistants, voice commands, and interactive dashboards will replace long, static texts, allowing users to ask questions and adjust privacy settings with ease. Instead of a one-time agreement, privacy settings will evolve based on user behaviour and preferences.

Enhancing Privacy in APIs, Cloud Services, and IoT Devices.

Web applications rely heavily on APIs, cloud storage, and IoT devices, each of which introduces new privacy challenges. APIs will need clearer permission structures to prevent unnecessary data access by third parties. Cloud services will implement stronger encryption and access controls, ensuring that user data remains protected even when shared between platforms. IoT devices—like smartwatches and home assistants—will need real-time privacy controls, allowing users to quickly turn off data sharing or restrict tracking.

Giving Users More Control Over Their Data.

Rather than forcing users to accept or reject an entire privacy policy, future web applications will offer granular control over data-sharing. Users will be able to decide exactly which data can be collected, for how long, and for what purpose. Privacy dashboards will allow users to revoke permissions at any time, and features like self-expiring permissions will prevent unnecessary long-term data storage. Instead of endless settings buried in menus, everything will be streamlined and accessible.

AI Transparency and the Right to Challenge Automated Decisions.

AI plays a massive role in data collection and decision-making, but how many people really understand how these algorithms work? Privacy policies will need to clearly explain AI-driven processes, including how user data is analysed and used. People will have the right to opt out of AI-driven decisions and even challenge automated judgments—whether it's a credit score, job application screening, or personalized ads. AI-powered privacy assistants will also help users navigate settings, ensuring they make informed choices.

Better Security Measures to Protect User Data.

With rising cyber threats, privacy policies will emphasize stronger security features. We will see widespread adoption of end-to-end encryption, biometric authentication, multi-factor security, and zero-knowledge encryption. Organizations will shift from simply responding to data breaches to implementing proactive security strategies that prevent them in the first place. Policies will outline these protections clearly, reassuring users that their data is safe.

Making Data Retention and Deletion Simple and Transparent.

Many users don't realize how long their data is stored—or that it's even being stored at all. Future privacy policies will make this more transparent by offering self-destructing data features and easy-to-use deletion options. Users will no longer have to go through endless customer support requests to delete their data; instead, they will have instant control over what stays and what gets erased. The "right to be forgotten" will become as easy as clicking a button.

Global Compliance Without Complexity.

As privacy regulations evolve worldwide—such as GDPR, CCPA, and India's PDPB—companies will need to comply with multiple legal frameworks. Future privacy policies will be designed to adapt automatically based on the user's location, ensuring legal compliance without complicating the user experience. Technologies like secure multiparty computation (SMPC) and homomorphic encryption will allow businesses to process sensitive data without actually "seeing" it, reducing risks while maintaining functionality.

BIBLIOGRAPHY

1 'California Consumer Privacy Act (CCPA)' (*State of California - Department of Justice - Office of the Attorney General*, 15 October 2018) <https://oag.ca.gov/privacy/ccpa> accessed 9 March 2025

2 'California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General' <https://www.oag.ca.gov/privacy/ccpa> accessed 9 March 2025

3 CDC, 'Health Insurance Portability and Accountability Act of 1996 (HIPAA)' (*Public Health Law*, 10 September 2024) <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html> accessed 9 March 2025

4 'Data Protection Impact Assessment (DPIA)' (*GDPR.eu*, 9 August 2018) <https://gdpr.eu/data-protection-impact-assessment-template/> accessed 9 March 2025

5 'Digital Personal Data Protection Act 2022/23' <https://www.dpdpa.in/> accessed 9 March 2025

6 'General Data Protection Regulation (GDPR) – Legal Text' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/> accessed 9 March 2025

7 '——' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/> accessed 9 March 2025

8 'Http://Www.Ftc.Gov/Ogc/Coppa1.Htm'

9 'LGPD Brazil - General Personal Data Protection Act' <https://lgpd-brazil.info/> accessed 9 March 2025

10 Mhaidli A and others, 'Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities' (2023) 2023 Proceedings on Privacy Enhancing Technologies 287

11 Nagarwal N, 'Privacy Policy and Data Protection Laws in India' (*LegalWiz.in*, 3 July 2020) <https://www.legalwiz.in/blog/privacy-policy-and-data-protection-laws-in-india> accessed 6 March 2025

12 'The PRC Personal Information Protection Law (Final): A Full Translation' (*China Briefing News*, 24 August 2021) <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/> accessed 9 March 2025

13 Thornton N, 'Privacy Policies: What They Are and Why They Matter' (*PrivacyEnd*, 30 August 2023) <https://www.privacyend.com/what-are-privacy-policies/> accessed 9 March 2025

14 van der Schyff K, Prior S and Renaud K, 'Privacy Policy Analysis: A Scoping Review and Research Agenda' (2024) 146 Computers & Security 104065

15 'What Does a Privacy Policy Need to Include?' (*TermsFeed*, 16 February 2025) <https://www.termsfeed.com/blog/privacy-policy-needs-to-include/> accessed 6 March 2025