Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Privacy in the Age of Digital Surveillance: Analyzing WhatsApp's Policy and Cybersecurity Implications

Khan Nazma Sohrab1*

[1*]*Research Scholar, Department of Law, Gujarat National Law University, Attalika Avenue Knowledge Corridor, PDPU Rd, Koba, Gujarat, India,* nazmaphd202022@gnlu.ac.in

ARTICLE INFO

Received: 18 Dec 2024

Revised: 16 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Introduction: Privacy is one area of great concern today, especially with the growing use of encrypted messaging platforms, in defining relationships in the more digital space. This paper critically examines the privacy policies of WhatsApp against the backdrop of evolving digital surveillance and international data protection frameworks such as the GDPR, CCPA, and LGPD.

Objectives: Evaluate WhatsApp's compliance with global and Indian data protection standards, focusing on cybersecurity threats related to metadata and surveillance, as well as regulatory responses, particularly the Indian Digital Personal Data Protection (DPDP) Act and Rules 2025.

Methods: A qualitative research methodology was used, focusing on policy analysis, case reviews, and regulatory documents. This includes assessing changes in WhatsApp's policy, examining breach incidents, and interpreting legal developments through doctrinal and comparative analysis.

Results: The study findings show that privacy concerns persist despite WhatsApp's end-to-end encryption, due to issues like metadata collection, unencrypted cloud backups, and spyware vulnerabilities. The 2021 policy update faced global backlash, highlighting failures in consent and data transparency. In India, the DPDP Act imposes strict obligations for user consent, breach notifications, and data rights.

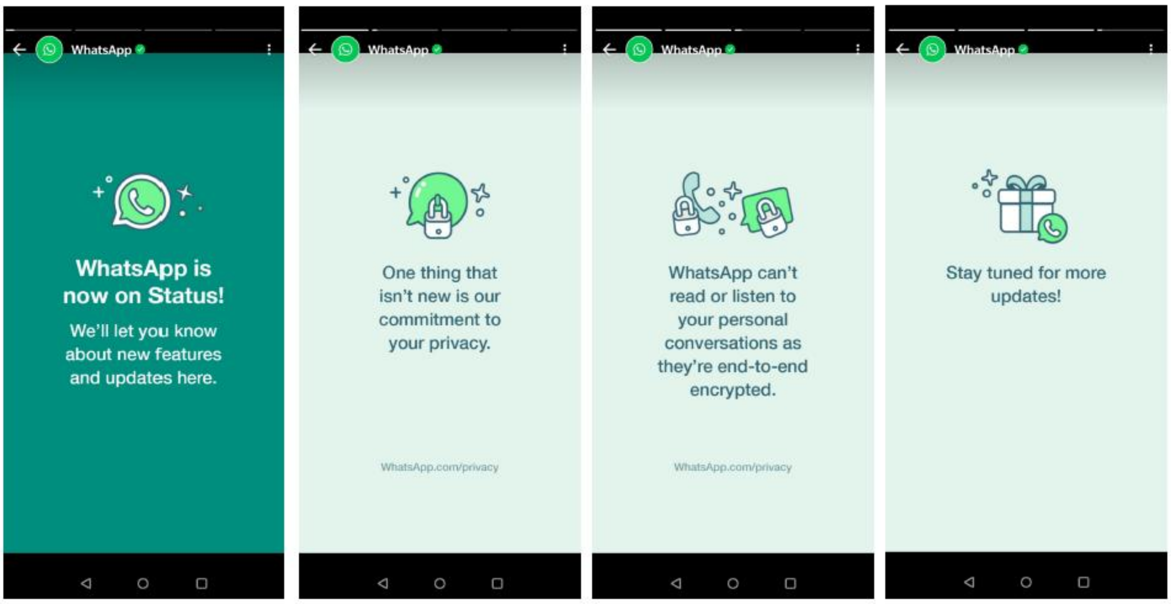
Conclusions: The study concludes that while WhatsApp meets encryption expectations, deeper issues persist. To foster digital trust, platforms should focus on user autonomy, transparency, and strong data protection. Regulatory reforms, such as India's DPDP Act, are crucial, but enforcement and public awareness, along with a balance between privacy and national security, must also progress.

Keywords: Cybersecurity, Data Protection, Digital Privacy, Metadata, Surveillance, WhatsApp.

INTRODUCTION

The Supreme Court recognized the Right to Privacy as a fundamental right in India with its landmark ruling in Justice K.S. Puttaswamy v. Union of India (2017). The judgment declared privacy as inherent to life and liberty under Article 21 of the Constitution (Satyanarayana, 2021). It essentially prepared the ground for the protection of one's personal autonomy, dignity, and informational privacy in the technological age. At present, with increased dependence on digital platforms, the definition of privacy should include digital privacy, demanding even more accountability from data collectors and platforms like WhatsApp (Vijay, et. al., 2023).

In today's digitally linked society, digital privacy is becoming a more important concern. Digital privacy pertains to an individual's rights regarding their personal data in an online context (Sur et al., 2021). As technology has advanced, so too have concerns regarding the collection, storage, and utilization of personal data. Digital privacy is particularly salient in the context of the proliferation of digital services that often gather extensive user data, frequently without explicit consent. This has led to the emergence of data protection laws and regulatory frameworks, such as the General Data Protection Regulation (GDPR) enacted in the European Union, along with similar initiatives being developed globally (Tiwari, 2024). Now the increased digital surveillance from state to private organizations is more focused on analyzing how digital platforms manage and secure data about users, so very critical ethical and legal issues arise (Perry, et. al., 2017).



WhatsApp is now on Status!

We'll let you know about new features and updates here.

One thing that isn't new is our commitment to your privacy.

WhatsApp.com/privacy

WhatsApp can't read or listen to your personal conversations as they're end-to-end encrypted.

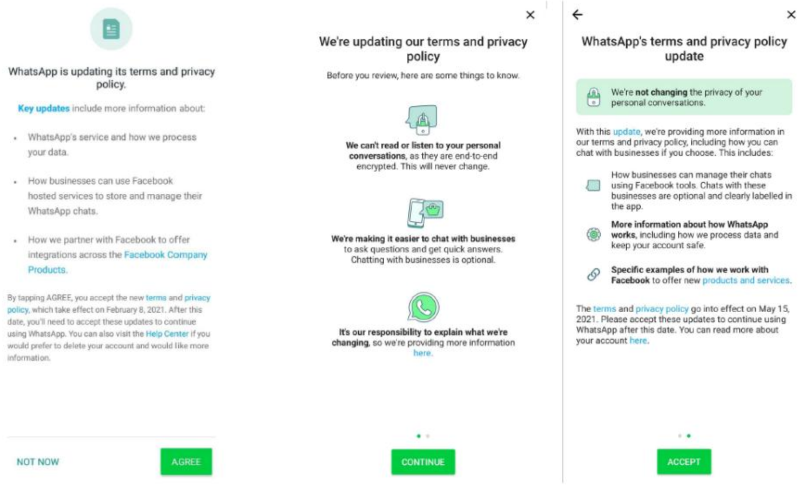
WhatsApp.com/privacy

Stay tuned for more updates!

Figure 1: WhatsApp's Status (24-hour ephemeral posts) to inform users about its upcoming privacy policy update

Source: WhatsApp

The popular and well-known app in the digital world with a large user database is WhatsApp. WhatsApp is truly among the most widely used communication platforms in the world, having about 2 billion users. From the get-go, being hailed as an encryption-oriented messaging app catering highly to user privacy, WhatsApp has laid its ground as a secure medium for personal and business conversations (Santos, et. al., 2018). The platform has undergone several updates over the years to bolster its security architecture. However, the acquisition by Facebook (now Meta) has raised serious questions regarding the degree of data-sharing between the two platforms. Users and regulators alike have raised concerns regarding whether WhatsApp's data-sharing ethos falls in line with the tenets of digital privacy given Meta's history of privacy scandals (Reis, et. al., 2020).



WhatsApp is updating its terms and privacy policy.

Key updates include more information about:

- WhatsApp's service and how we process your data.
- How businesses can use Facebook hosted services to store and manage their WhatsApp chats.
- How we partner with Facebook to offer integrations across the Facebook Company Products.

By tapping AGREE, you accept the new terms and privacy policy, which take effect on February 8, 2021. After this date, you'll need to accept these updates to continue using WhatsApp. You can also visit the Help Center if you would prefer to delete your account and would like more information.

(a) January 4 update notification

We're updating our terms and privacy policy

Before you review, here are some things to know.

We can't read or listen to your personal conversations, as they are end-to-end encrypted. This will never change.

We're making it easier to chat with businesses to ask questions and get quick answers. Chatting with businesses is optional.

It's our responsibility to explain what we're changing, so we're providing more information here.

WhatsApp's terms and privacy policy update

We're **not changing** the privacy of your personal conversations.

With this update, we're providing more information in our terms and privacy policy, including how you can chat with businesses if you choose. This includes:

How businesses can manage their chats using Facebook tools. Chats with these businesses are optional and clearly labelled in the app.

More information about how WhatsApp works, including how we process data and keep your account safe.

Specific examples of how we work with Facebook to offer new products and services.

The terms and privacy policy go into effect on May 15, 2021. Please accept these updates to continue using WhatsApp after this date. You can read more about your account here.

(b) February 18 update notification

Figure 2: Two versions of WhatsApp's in-app pop-up notification about its privacy policy update

Source: Griggio, et. al., (2022).

This study is intended to critically analyze the privacy policies of WhatsApp to assess their compliance with international data protection standards. The study would assess to what extent digital surveillance affects the privacy of WhatsApp users being used to analyze how the data-sharing practices of the platform can lead to cybersecurity risks. By doing forge, this study would be relevant in the bigger discourse on the subject of digital privacy in the times of surveillance capitalism and growing scrutiny under the law.

Research Question

Q1. How do WhatsApp's privacy policies compare with established global data protection regulations, and to what extent do they comply with these standards?
Q2. What impact does digital surveillance have on the privacy and security of WhatsApp users, and how can this be evaluated using secondary benchmark data?
Q3. How can the cybersecurity risks associated with WhatsApp's data-sharing practices be effectively assessed and mitigated?
Q4. How have WhatsApp's privacy policies evolved in response to growing digital surveillance challenges, and what policies and recommendations can be proposed to address these challenges?

Research Objective

Obj1. To explore the alignment of WhatsApp's privacy policies with established global data protection regulations and assess the extent of compliance.

Obj2. To evaluate the impact of digital surveillance on the privacy and security of WhatsApp users using secondary benchmark data.

Obj3. To assess and identify effective strategies for mitigating cybersecurity risks associated with WhatsApp's data-sharing practices.

Obj4. To observe the evolution of WhatsApp's privacy policies in response to digital surveillance challenges and propose suitable policy recommendations.

RESEARCH METHODOLOGY

This study includes a qualitative approach aimed at assessing critically the development of privacy policies for WhatsApp, given the growing threats to cybersecurity and the rise of digital surveillance challenges. The study is built on an exhaustive review of secondary data sources, including but not limited to official policy documents released by WhatsApp, important international data protection laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), reports from government and regulatory authorities, scholarly journal articles, and published studies on cyber security cases. Adopting a generally comparative analysis approach, the study provides an appraisal of how far concerning data handling practices WhatsApp is comparable to the global standards of privacy while pointing out areas of compliance and existing gaps in policy and law in this regard. Case studies are being used to show the example of practical insights through the analysis of some real examples such as breaches of data, incidences of surveillance, and violations of privacy related to WhatsApp, therefore demonstrating the true dangers to which any user is exposed in the digital communication space. An assessment will also be done in terms of regulation towards identifying how far the government agencies, courts, or other legal institutions scrutinize, respond, and direct upon the privacy practices of WhatsApp, including the investigation of regulatory inquiries, legal precedents, and other forms of enforcement actions made via different jurisdictions. With this methodological matrix, a comprehensive understanding of the interplay between privacy regulations, evolution in corporate policies, and cybersecurity issues would contribute eventually to improved and industry-related policy recommendations on user data security and mitigation of surveillance hang-ups.

TIMELINE OF WHATSAPP'S PRIVACY POLICY CHANGES

From 2009 onward, WhatsApp has faced many changes in privacy policies, largely influenced by technological and regulatory developments or corporate decisions. Initially thought of as a private messaging service, the emphasis was always on secure communication, with the least data collection (Nene, 2017). That attention began to be lost when it was acquired by Facebook in 2014, and data privacy and security issues started to be raised, thus starting the policy changes that would characterize its stance on privacy (Trautman, 2019). In 2016, WhatsApp made end-to-end encryption the default for any message, call, photo, or video communication. Only the sender and recipient could see the content of any communication, which was widely hailed as a landmark step toward digital privacy and user security. However, that same year, WhatsApp changed its privacy policy to give more data to Facebook for ad targeting, friend recommendations, and analytics-a move that has come under fire, with several users and privacy advocates raising concerns regarding the possibility of misuse of the personal information (Rösler, et. al., 2018).

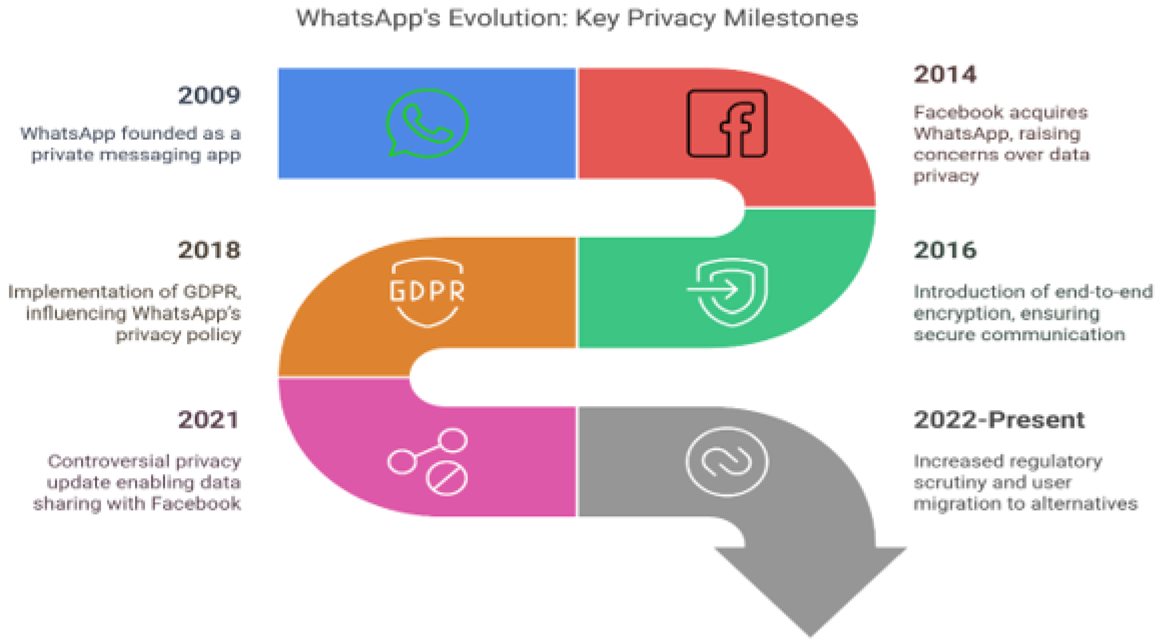
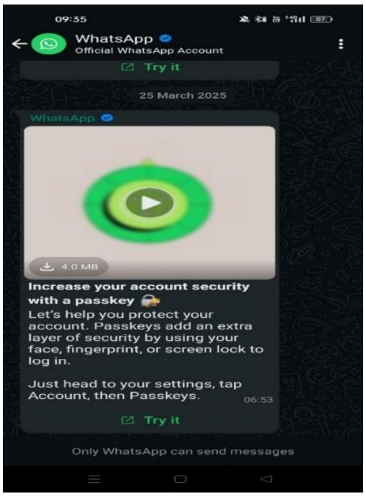

WhatsApp's Evolution: Key Privacy Milestones
2009
WhatsApp founded as a private messaging app
2014
Facebook acquires WhatsApp, raising concerns over data privacy
2018
Implementation of GDPR, influencing WhatsApp's privacy policy
GDPR
2016
Introduction of end-to-end encryption, ensuring secure communication
2021
Controversial privacy update enabling data sharing with Facebook
2022-Present
Increased regulatory scrutiny and user migration to alternatives

Figure 3: Evolution of WhatsApp

Source: Self-prepared by author

WhatsApp has had to change the way it presents and uses user privacy information by implementing the General Data Protection Regulation (GDPR), which started back in 2018. Most importantly, WhatsApp had to comply with much stricter data protection laws, especially in the European Union. WhatsApp has since assured users in Europe that it would limit the data-sharing practices according to the restrictions of the GDPA. Still, the rest of the world has gone about its work, and this has further fueled suspicions concerning user privacy and transparency (Rancati, et. al., 2019). The most controversial privacy update occurred in January 2021 when WhatsApp announced changes to its terms of service, requiring users to accept certain data from Facebook. The update gave rise to widespread uproar, with users fearing that WhatsApp would share their private messages and personal details with Facebook for advertising and commercial purposes. While WhatsApp clarified that encrypted personal messages were unaffected by the update, the public outcry prompted a mass migration of users to other messaging apps, such as Signal and Telegram. Governments and regulatory bodies in several countries scrutinized the update; thus, WhatsApp announced the postponement of the rollout to accommodate public regard (Griggio, et. al., 2022).

WhatsApp has been under greater scrutiny from regulators since 2022 for its data-sharing policy. Different governments and privacy watchdogs have raised questions as to their compliance with global data protection standards, leading to legal challenges and fines in several jurisdictions. As awareness of digital privacy has risen, many users still seek alternative apps that provide stronger privacy provisions against WhatsApp. The market moved to more privacy-oriented messaging services, indicating a growing demand for transparency and control over personal data in the digital age (Olaniyi, et. al., 2023). The transformational time of WhatsApp in privacy policy changes is one problem as it is a broader scenario with digital platforms. Some of the problems are addressing business interests against user privacy. However, with the growing outcry over digital surveillance and the connective's data security, this former norm of WhatsApp's privacy policy concerning the future shall not have a free run under the eyewatch of users and regulators around the world (Henkoglu, 2022).



Increase your account security with a passkey 🔐
Let's help you protect your account. Passkeys add an extra layer of security by using your face, fingerprint, or screen lock to log in.

Just head to your settings, tap Account, then Passkeys.

Only WhatsApp can send messages

Figure 4: WhatsApp sending message to increase personal security

Source: WhatsApp

THEORETICAL FRAMEWORK

a) Surveillance Capitalism Theory (Inventor: Shoshana Zuboff)

Zuboff's Surveillance Capitalism Theory frames a critique that reveals how the commercialization of personal data occurs in the digital age. In terms of this theory, companies and digital platforms extract, analyze, and monetize behavioral information about users even without their explicit consent (Zuboff, 2022). In this context of the unusual policy changes in WhatsApp, Surveillance Capitalism Theory explains how data practices go beyond assessable communication services and influence consumer behavior and market dynamics. Privacy has become a commodity in these digital markets, where user trust is exploited to make some money with targeted advertising and predictive analytics. The theory further emphasizes the opposing tension of promised secure communication and systematic surveillance (Chai, et. al., 2023). The theory brings interesting insights into a host of cybersecurity threats and more general privacy under siege from digital surveillance through the investigation of these mechanisms. Implications of this nature then demand stronger regulation and practices for gaining informed consent from users (Koczur, 2022).

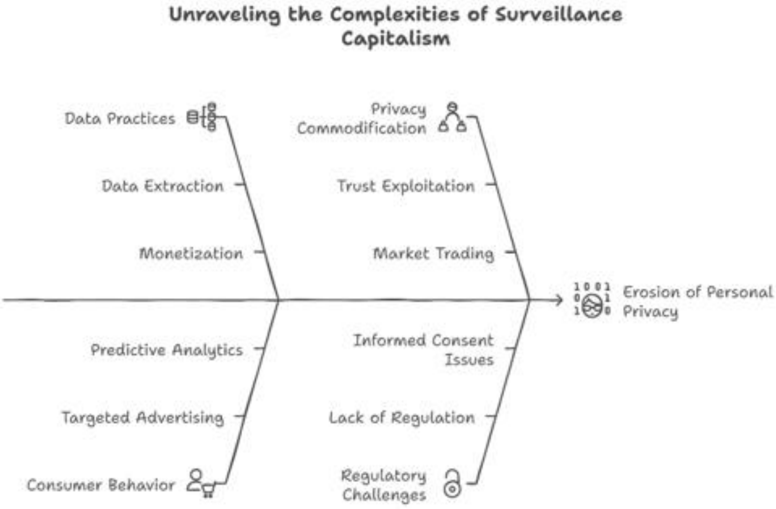


Figure 5: Unravelling the complexities of Surveillance Capitalism

Source: Self-prepared by author

b) Privacy Paradox Theory (Inventor: Alan Westin)

The Privacy Paradox is a theory attributed to Alan Westin, discussing the contradictory position held by individuals regarding their expressed worries over privacy, versus their actions under the umbrella of the digital era (Alić, et. al., 2023). The theory states that while users often shout for data protection, they willingly trade personal information for convenience and contact with others. In the case of WhatsApp's privacy policy, the Privacy Paradox Theory reveals a gap between users' expectations of private services and the forms that data collection takes behind the digital services (Adorjan, et. al., 2019). The idea behind this is that consent is often acquired to great effect yet always in a manner so complex that it leads to unintended data sharing and surveillance. Redressing the prevailing privacy norm with a need for transparency in policies and real user control over personal information is the task given to the theory. With its accent on the growing forms of digital surveillance, Privacy Paradox Theory offers an opportunity to reconceptualize cybersecurity frameworks whereby actual user behavior clashes with professed and true concerns for privacy, putting in place a more balanced world. That says- this is urgent and needs to get done immediately and in good measure (Li, 2024).

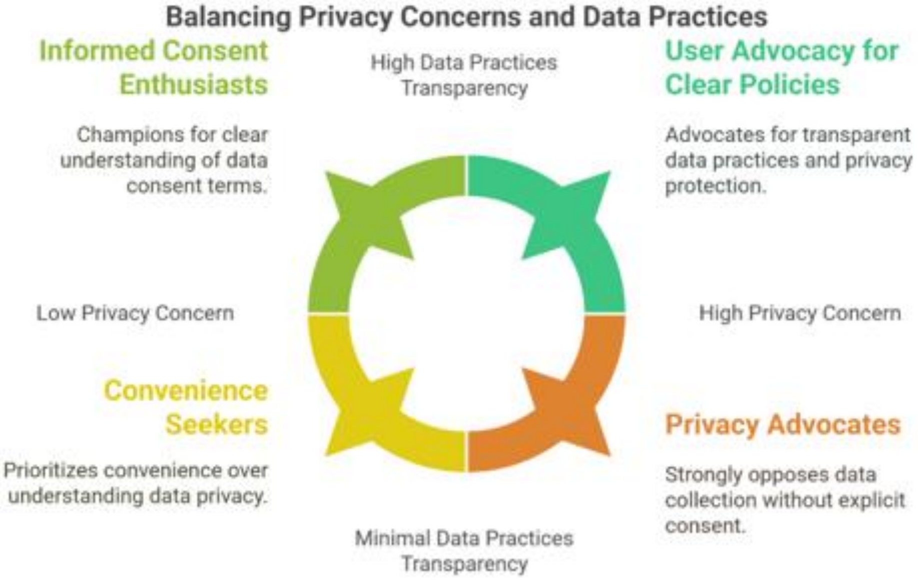

Balancing Privacy Concerns and Data Practices
Informed Consent Enthusiasts
Champions for clear understanding of data consent terms.
High Data Practices Transparency
User Advocacy for Clear Policies
Advocates for transparent data practices and privacy protection.
Low Privacy Concern
High Privacy Concern
Convenience Seekers
Prioritizes convenience over understanding data privacy.
Privacy Advocates
Strongly opposes data collection without explicit consent.
Minimal Data Practices Transparency

Figure 6: Balancing Privacy Concerns & Data Practices

Source: Self-prepared by author

c) Zero-Trust Security Model (Inventor: John Kindervag)

The Zero-Trust Security Model founded by John Kindervag redefines cybersecurity as one that does not consider the existence of an internal trusted network. According to this theory, all access claims must be verified and validated both inside and outside an organization's perimeter, before permission is granted (Jena, 2023). The Zero-Trust Model, within WhatsApp's context and along the glittery avenues of privacy policies and cybersecurity protocols, challenges the assumption that an endpoint secured harbors safety. As such, it calls for a continuous authentication mechanism, strict access to all resources, and micro-segmentation, thereby weakening the chances of successful attack scenarios (Edo, et. al., 2022). In the digital surveillance era, the model is especially relevant, where data is repeatedly targeted by advanced threats. The theory promotes a dynamic and resilient security posture, assuming that no inherent trust prevails in the design, adaptable to the changing nature of attack vectors. This proactive approach against potential vulnerabilities serves to reinforce the other aspects of laying a solid foundation for cybersecurity practices in safeguarding personal data and privacy in today's interconnected digital space. In ensuring protection for all personal data against various vulnerabilities, including environmental threats, an emphasis must be placed on building such measures into any system (Olaniyi, 2023).

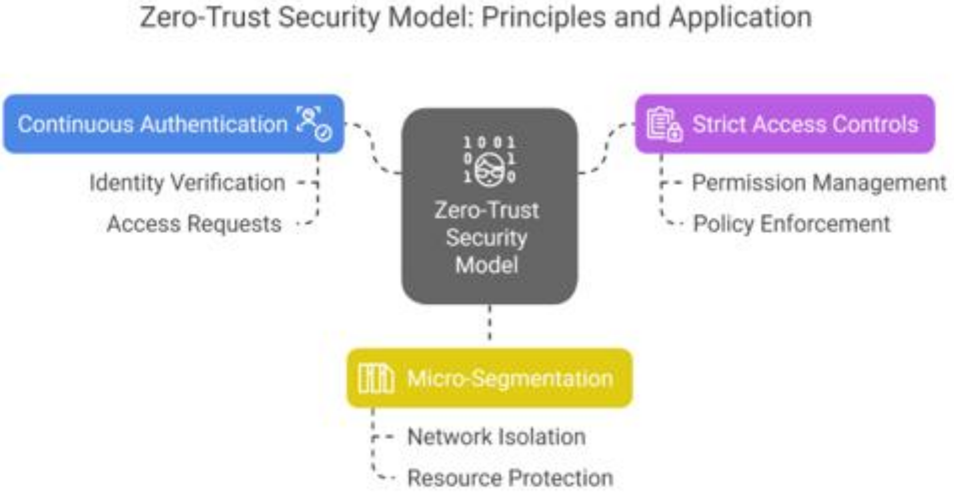


Figure 7: Zero-Trust Security Model

Source: Self-prepared by author

CYBERSECURITY IMPLICATIONS OF WHATSAPP'S PRIVACY POLICY

Data Privacy and Cybersecurity Risks

WhatsApp's privacy policy poses threats of grave concern to the user as they are subjected to serious data privacy and cybersecurity risks. The platform collects data in broad strokes: an entire purchase history, location, device identifiers, and activity logs, which may be sold to third-party marketing companies for behavioral profiling. Backups of chats saved on Google Drive or iCloud are unencrypted by default and prone to being snatched or illegally accessed by cloud providers. At the same time, hackers never miss an opportunity to exploit the same vast numbers of users by engaging in phishing, distributing harmful attachments, and coming up with new "broken link" techniques to steal passwords and spread malware.

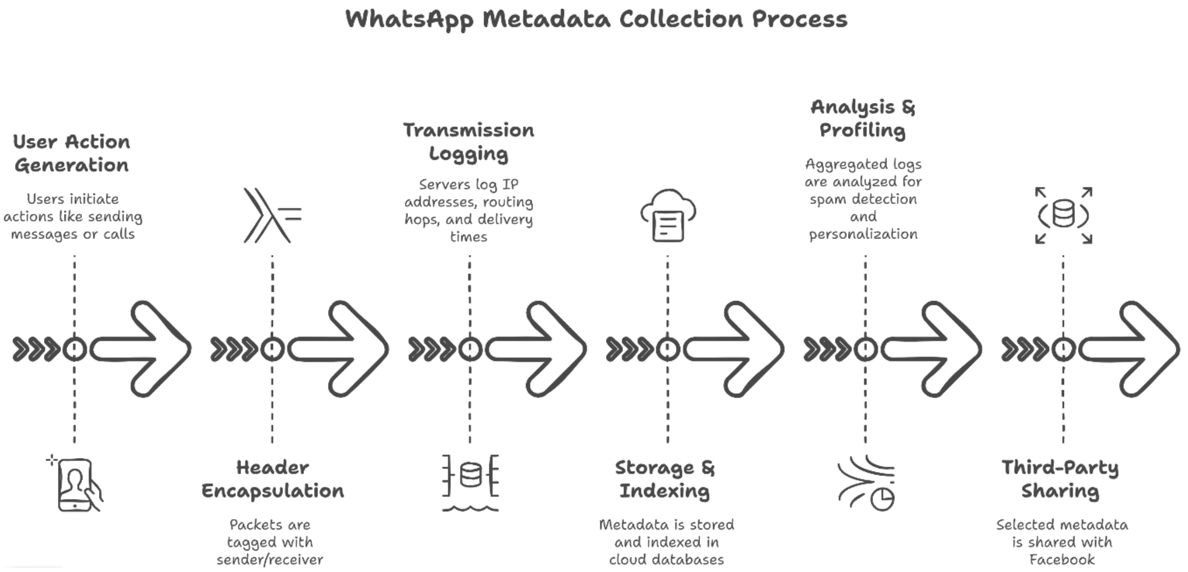

WhatsApp Metadata Collection Process
User Action Generation
Users initiate actions like sending messages or calls
Header Encapsulation
Packets are tagged with sender/receiver
Transmission Logging
Servers log IP addresses, routing hops, and delivery times
Storage & Indexing
Metadata is stored and indexed in cloud databases
Analysis & Profiling
Aggregated logs are analyzed for spam detection and personalization
Third-Party Sharing
Selected metadata is shared with Facebook

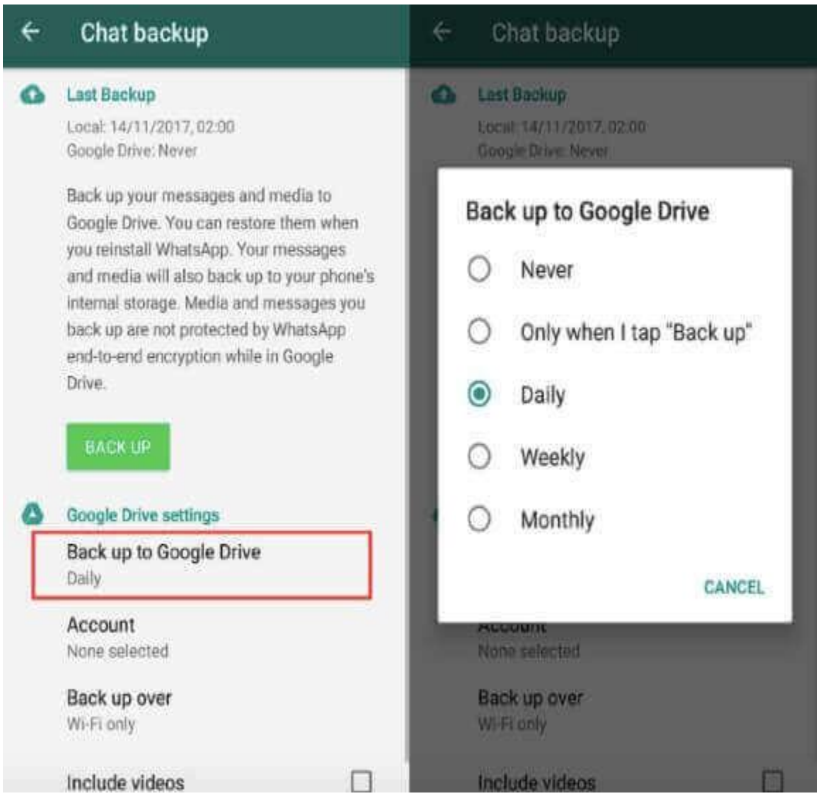
Figure 8: WhatsApp Metadata Collection Process

Source: Self-prepared by author

Metadata of all messages—sender and receiver phone numbers; timestamps, device, and network identifiers—is kept by WhatsApp without revealing the content of messages. Plain text still contains metadata despite the fact that the metadata is protected from view by end-to-end encryption guarding chat content, thus allowing the potential for traffic analysis attacks inferring social graphs, movement patterns, and peak activity periods. Such collected and stored metadata may contain profile information, IP addresses, and frequency of communication, which can further be built together into constructing very detailed user profiles for surveillance or targeted marketing.

Cloud Backups and Vulnerabilities: unencrypted Google Drive / iCloud

Conversations are, by default, somewhat insecurely backed up to either Google Drive (Android) or iCloud (iOS) by WhatsApp, which makes the entire conversation archive completely accessible to cloud providers or any possible lawfully sanctioned access. Security analyses demonstrate that the backups can either be downloaded directly from the user's cloud account or be intercepted if a credentials breach occurs, meaning that the backs are effectively outside of WhatsApp's in-transit encryption protection. End-to-end encrypted backups were introduced by WhatsApp as an optional feature in September 2021, but uptake has remained low, with the opt-in setting buried deep within app menus. Recent studies indicate that the vast majority of users remain at risk since encrypted-backup settings are neither default-configured nor prominently marketed.



Local: 14/11/2017, 02:00
Google Drive: Never

Back up your messages and media to Google Drive. You can restore them when you reinstall WhatsApp. Your messages and media will also back up to your phone's internal storage. Media and messages you back up are not protected by WhatsApp end-to-end encryption while in Google Drive.

Back up to Google Drive
Daily

Account
None selected

Back up over
Wi-Fi only

Include videos □

Back up to Google Drive

○ Never
○ Only when I tap "Back up"
● Daily
○ Weekly
○ Monthly

Figure 9: WhatsApp Backup

Source: Self-prepared by author

Phishing and Malware Attacks: common vectors and exploited loopholes

Phishing scams on WhatsApp typically involve impersonation of trusted contacts or institutions, and some of their common tactics include using urgency or fear to trick users into clicking links or divulging personal data. Beyond this social engineering tactic, attackers exploit the application vulnerabilities, the most recent critical one being WhatsApp for Windows, by using crafted file attachments to execute arbitrary code, having endpoint integrity under threat. This was disclosed in April 2025 as CVE 2025 30401: a spoofing that allowed remote code execution after Windows users opened maliciously altered files. The latest added complexity to broken link attacks is that they exploit previewing features, which circumvent URL scanning defenses and lead to a silent installation of spyware. High-value phishing campaigns targeting enterprises serve as examples where threat actors use WhatsApp channels to harvest credentials and induce advanced persistent threats. Such a large number of users on WhatsApp makes it fertile training ground for social engineering and malware campaigns. The summary of attack waves observed in this user space is shown in Table 1, indicating the year of attack, the underlying issue exploited, and how detection or mitigation is based on metadata or adjunct measures.

Table 1. Phishing & Malware Attack Summary

Year	Attack Vector	Core Issue / Exploit	Metadata-Driven Detection & Mitigation	Additional Countermeasures	Citations
2021	Credential-phishing via SMS-links	Impersonation of trusted contacts; urgent "account compromised" lures	Flag unusual link-click patterns (e.g. high volume from atypical hours or geolocations)	URL-filtering, user-awareness prompts, two-step verification	Desolda, G., Ferro, L., Marrella, A., Catarci, T., & Costabile, M. (2021), Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021)
2022	Malicious Android APK distribution	Remote code execution via sideloaded apps	Detect anomalous file-size/distribution metadata; geolocation mismatches between download origin & user profile	Enforce APK signing checks, opt-in scan of media attachments	Erfina, A., Hidayat, R., Rafli, R., Rizaldi, R., Maulana, R., & Falentino, T. (2023), Sudjayanti, S., & Hamdani, D. (2024)
2023	Spam voice-call phishing	Social-engineering through repeated "missed calls" directing to scam SMS	Monitor high-frequency call patterns from single numbers; threshold-based rate-limiting	Built-in spam-call filter, caller-ID verification	Chamorro-Atalaya, O., Aguilar, M., Candia-Quispe, W., Roman-Gonzalez, A., Cruz-Telada, Y., Suarez-Bazalar, R., & Arévalo-Tuesta, J. (2023), Hashmi, S., George, N., Saqib, E., Ali, F., Siddique, N., Kashif, S., Ali, S., Bajwa, N., & Javed, M. (2023)
2024	"Broken-link" malware	Abuse of link-preview to bypass URL-scanning defenses	Compare preview metadata (title, domain) versus actual redirect chain	Harden preview sandbox, strip metadata raw URLs	Liu, Y., Tantithamthavorn, C., Li, L., & Liu, Y. (2021), Li, D., & Li, Q. (2020)

2025	CVE-2025-30401: Windows remote code execution	Crafted file attachments launching arbitrary code on Windows desktop	Track anomalous file-hash and timestamp metadata; quarantine based on reputational signals	Prompt security-patch reminders, integrated file-scanner on download	Kalpana, C., Rushikesh, N., & Srikanth, A. (2023), Kalpana, C., Rushikesh, N., & Srikanth, A. (2023)

NATIONAL SECURITY DEMANDS FOR CHAT ACCESS

Government Demands for WhatsApp Chat Access

Table 2: Government Demands for WhatsApp Chat Access – Controversies, Reasons, and Outcomes

Year	**Country**	**Triggering Controversy / Reason**	**Government Demand**	**WhatsApp's Response**	**Citations**
2017	**UK**	Manchester Arena Bombing – attacker used WhatsApp minutes before the blast	UK Home Secretary demanded access to encrypted chats for terror investigations	Refused; stated breaking E2EE would risk security of all users	Endeley, R. (2018), Vamsi Krapa, S.Prayla Shyry, M.Rahul Sai Krishna (2019)
2018	**Australia**	Child exploitation & terror threats	Enacted Assistance and Access Act mandating technical capability notices	Expressed concern; joined global industry coalition opposing encryption backdoors	Nicol, S., Harris, D., Kebbell, M., & Ogilvie, J. (2021), Hunn, C., Spiranovic, C., Prichard, J., & Gelb, K. (2020)
2019	**India**	Mob lynchings, misinformation during elections	Proposed traceability clause in IT Rules (Rule 4)	Filed legal case in Supreme Court; maintained that traceability breaks encryption	Bhat, M., Bajaj, V., & Kumar, S. (2020), Nojeim, G., & Maheshwari, N. (2020)
2020	**Brazil**	Covid-19 disinformation, political propaganda via WhatsApp groups	Supreme Court order to identify origins of fake news	Partially complied (blocking accounts); challenged order on grounds of free speech and encryption	Soares, F., Recuero, R., Volcan, T., Fagundes, G., & Sodré, G. (2021), Rossini, P., & Kalogeropoulos, A. (2023)
2021	**Germany**	Neo-Nazi online coordination, extremist groups organizing on chat platforms	Proposal to regulate messenger apps & mandate content traceability	Warned of mass surveillance risk; launched privacy outreach campaigns	Khrishkevich, T. (2022), Arestova, E., & Borbat, A. (2023)
2022	**USA**	January 6 Capitol Riots – coordination suspected on encrypted platforms	Lawmakers called for platform accountability and backdoor access	Highlighted commitment to E2EE; Meta emphasized cooperation via	Bucci, R., Kirk, D., & Sampson, R. (2022), Challacombe, D., & Patrick, C. (2022)

				metadata & lawful emergency disclosures	
2023	**UK**	Online child exploitation (via Operation Hydrant & NCA reports)	Reintroduction of “Online Safety Bill” to mandate scanning of private chats	Threatened to leave UK market if compelled to break encryption; supported child safety via reporting tools	Cooray, M., Rajuhan, I., & Adnan, W. (2023), Quayle, E. (2020)
2024	**India**	Manipur violence and hate speech amplification through private messaging	Renewed pressure for traceability and faster content takedown mechanisms	Reiterated encryption stance; offered transparency reports and AI-based flagging of harmful content	Sahoo, N. R., Beria, G. P., & Bhattacharyya, P. (2024), https://economictimes.indiatimes
2025	**Brazil & EU**	Election misinformation, AI-generated deepfakes spread via encrypted groups	Demand for content traceability, message origin tags, and content identification	Pushed back with privacy impact studies; offered to enhance metadata sharing under strict legal oversight	dfrlab.org, weforum

Governments' demand for chat access has steadily increased ever since these technologies came into the limelight, with perceived threats ranging from terrorism and misinformation to hate speech and online exploitation. Each incident, whether the Manchester bombing (UK, 2017), mob lynchings in India (2019), or the Capitol Hill riots (US, 2022), has put end-to-end encryption on the radar of governments as an impediment to national security and legal investigations. The company has resisted formidable pressure to compromise its encryption but instead has increased transparency, assisted with disclosures of metadata, and provided non-intrusive safety tools. WhatsApp's resistance is not only based on technical grounds and ethics but also based on its deep apprehensions that once backdoors are created, they will be used against its users by malicious hackers and authoritarian regimes.

“Backdoors” Controversy in Encryption for Law Enforcement

Governments all over the world, and especially under the UK Investigatory Powers Act, Australia's Assistance and Access Act, and India's IT Rules, have repeatedly urged encrypted messaging services to create "backdoors" for law enforcement to get access to plaintext chats (Endeley, 2019). Proponents argue that such access is essential for counterterrorism, child sexual exploitation investigations, and prosecutions for organized crime. The critics, however, warn that any built-in decryption key would create a situation where the backdoor could be misused not only by the states but also by criminal hackers and authoritarian regime leaders. Tech companies-anywhere between Apple to WhatsApp's parent, Meta-states that when a backdoor exists, it cannot be selectively controlled, and its existence ultimately breaks the security and privacy for millions of users (Chen, et. al., 2022). Groups of civil society and cryptographers went against such mandatory access, suggesting instead for lawful intercept frameworks that do not rely on weakening core E2EE protocols but only use metadata and active cooperation approved by the courts (Haddad, et. al., 2024).

WhatsApp’s Official Responses to Surveillance Requests

WhatsApp deals with demands for government access to data via a dedicated Law Enforcement Response Team (LERT), which reviews each request against local laws and company policy (Durrant et al., 2022). In addition, Meta's Transparency Center publishes biannual reports on the number of requests received, the percentage met, and the type of data disclosed, which mainly involves user metadata but never message content (Crystal-Ornelas et al., 2022).

WhatsApp may have decided to speed up its minimal metadata disclosures, such as account registration data, in emergencies, while also building internal checks to deny overly broad or non-judicial demands. Such a method would comply with legislation even as it firmly entrenches in technical commitment to end-to-end encryption (Manji, et. al., 2021).

THE ROLE OF END-TO-END ENCRYPTION

E2EE is the principal technology for WhatsApp against eavesdropping and content tampering. Messages are encrypted on the sender's device and decrypted on the receiver's device;, hence no one in between— including WhatsApp's servers—has the possibility to view a message or change its contents (Maglaras, et. al., 2022).

How E2EE Protects Message Content

When a user sends a message, WhatsApp's client:

- Every communication on a cell phone would require a private session key protection mechanism.
- Signal Protocol uses the key to encrypt the message payload (text, media, attachments).
- Apart from sending ciphertext and associated metadata, the WhatsApp server does not do anything.
- Transports the ciphertext to the recipient, having the corresponding decryption key stored in the device (Shen, 2021).

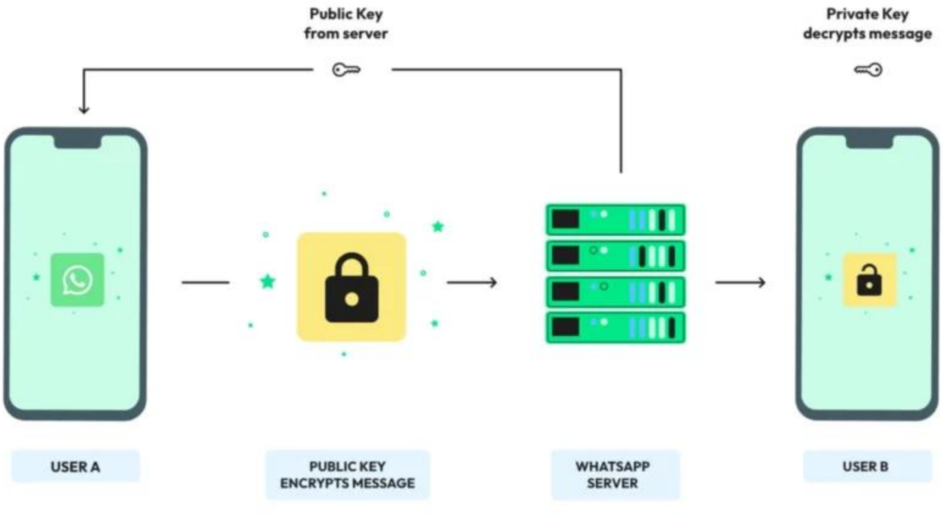


Figure 10: WhatsApp E2EE

Source: Self-prepared by author

The server cannot intercept the message due to cryptographic impossibility, as the decryption keys never leave these two endpoints. Even if the infrastructure is compromised, plaintext cannot be recovered by attackers without possession of the users' private keys (Santos, et. al., 2018).

Limitations: Compromised Backups & Spyware Threats

- **Unencrypted Cloud Backups:** Until late 2021, WhatsApp chat backups on Google Drive (Android) and iCloud (iOS) remained unencrypted. Hence, an adversary gaining access to a user's cloud account could download entire conversation archives in plaintext and thus undermine encryption in transit (Bawake, et. al., 2023).
- **Client-Side Compromise:** End-to-end encryption does not protect messages after decryption on a device. Advanced spyware organisms, that are installed with the help of a zero click exploit, can harvest messages, media, and even encryption keys directly from someone's handset (Limoncelli, 2023).

Table 3. Case Studies of Client-Side Attacks on WhatsApp

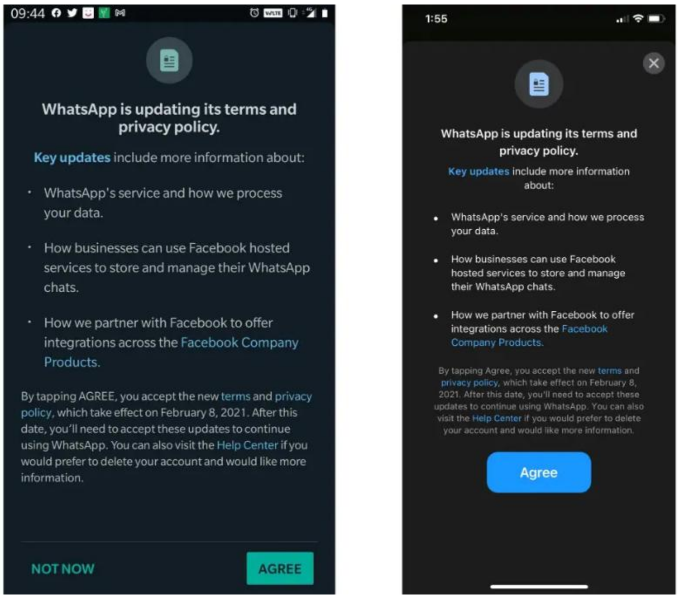
Year	Spyware / Attack	Exploit Mechanism	Targets & Impact	E2EE Bypass Vector	Source
2019	Pegasus (NSO Group)	CVE-2019-3568: zero-click buffer-overflow in WhatsApp's VoIP stack	~1,400 users—including journalists and dissidents—remotely infected; full exfiltration of chats & media	Remote code execution on device, before decryption	NVD CVE-2019-3568 NIST National Vulnerability DatabaseLog in or sign up to view; Reuters—NSO liable The Hacker News
2020	KISMET (NSO Group)	Invisible zero-click iMessage exploit chain ("Kismet") leveraged to deploy Pegasus-style spyware	36 Al Jazeera journalists and staff targeted; covert data extraction	Zero-interaction compromise of OS, uninstallable by user	Trend Micro / Citizen Lab summary Trend Micro, citizenlab.ca
2021	Predator Files (Cytrox / Intellexa)	Malicious video file delivered via WhatsApp; exploited unpatched media-parser vulnerability	High-value targets (e.g., Jeff Bezos) exfiltrated gigabytes of personal data	Execution of arbitrary code post-download, before display	Citizen Lab: Pegasus vs Predator The Citizen Lab, blog. Talosintelligence .com
2023	Pegasus "Triple Threat" updates	Three distinct zero-click chains against iOS 15 & 16 for remote installation of updated Pegasus modules	Broad targeting of dissidents, lawyers, corporate executives globally; continued stealth surveillance	Multiple OS-level zero-click vectors, undetectable by E2EE	Citizen Lab: Triple Threat The Citizen Lab, citizenlab

As highlighted in Table 3, E2EE secures messages while in transit, but this protection does not extend to attacks on the endpoints of compromise. This could be via vulnerabilities in cloud backup and the capability of sophisticated zero-interaction spyware.

KEY CHANGES IN WHATSAPP'S PRIVACY POLICY

Overview of the 2021 Update

On January 4, 2021, WhatsApp came up with a new updated Privacy Policy, which required the user to accept the wider sharing of data with its parent company, Facebook. Significantly, the new terms clarify that business account chat and metadata, such as phone number, transaction details, device identifiers, and usage data, might go to Facebook's advertising and analytics infrastructure. The change does not affect personal messages between individual users; yet, there was a major misconception among most people who believed that their chat content was subject to sharing. To implement the new policy, WhatsApp brought in-app display banners and full-screen prompts, requesting acceptance of the terms before May 15, 2021, or lose access to them. A detailed FAQ page emphasized that end-to-end encryption of personal messages remains intact, to which these banners were appended with "Learn More" links directing users. Critics contended that the deadline and limited opt-out options of business data sharing have violated principles of free and informed consent, thereby prompting antitrust scrutiny in several jurisdictions (Talwar, et al., 2022).



09:44

WhatsApp is updating its terms and privacy policy.

Key updates include more information about:

- WhatsApp's service and how we process your data.
- How businesses can use Facebook hosted services to store and manage their WhatsApp chats.
- How we partner with Facebook to offer integrations across the Facebook Company Products.

By tapping AGREE, you accept the new terms and privacy policy, which take effect on February 8, 2021. After this date, you'll need to accept these updates to continue using WhatsApp. You can also visit the Help Center if you would prefer to delete your account and would like more information.

NOT NOW AGREE

1:55

WhatsApp is updating its terms and privacy policy.

Key updates include more information about:

- WhatsApp's service and how we process your data.
- How businesses can use Facebook hosted services to store and manage their WhatsApp chats.
- How we partner with Facebook to offer integrations across the Facebook Company Products.

By tapping Agree, you accept the new terms and privacy policy, which take effect on February 8, 2021. After this date, you'll need to accept these updates to continue using WhatsApp. You can also visit the Help Center if you would prefer to delete your account and would like more information.

Agree

Figure 11: WhatsApp updating terms

Source: Self-prepared by author

Alongside that, WhatsApp made some major updates to its Business APIs by introducing interactive message templates like call-to-action buttons and quick reply options for conducting commerce and customer support on the platform. Now, companies could send order confirmations, shipment information, and appointment reminders via WhatsApp with the metadata from these interactions feeding into Facebook's wider business intelligence tools. This drive toward monetization drove home WhatsApp's strategy of using its two-billion-strong user base for enterprise messaging services (Hari & Abdulla, 2023).

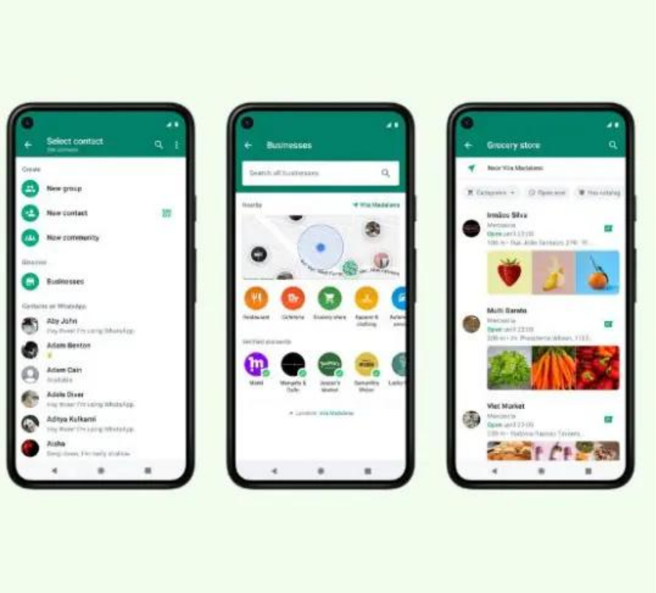


Figure 12: WhatsApp Business

Source: Self-prepared by author

User Backlash and Mass Migration

- **Decline in Global Trust and Media Reaction:** The big change in policies were then dubbed a “privacy betrayal,” and the tech and mainstream media further inflamed the frenzy with headlines proclaiming WhatsApp was now “giving” user data to Facebook. The rate of app store ratings went down drastically: Ratings from the Google Play Store for WhatsApp were lowered from 4.3 to 3.3 stars in a matter of days, while the Trustpilot rating fell from “Excellent” to “Poor”- all by mid-January, 2021 (Kalogeropoulos & Rossini, 2025).
- **Surge in Signal and Telegram Adoption:** The week after WhatsApp's announcement of the deadline on May 15, downloads skyrocketed for 4,200 percent in Signal compared to the previous week. That figure would translate to about 7.5 million installations, while Telegram was up by over 5.6 million downloads. Both apps cite privacy as their main selling point, with Signal's model as a non-profit and Telegram's secret chat option being a stark contrast to the Facebook associated WhatsApp foundation (Romero-Saritama, et al., 2025).

WhatsApp has come under sustained and intense scrutiny and has therefore set out a large FAQ on its website, last updated in May 2024, to dispel myths: it reiterated that only metadata pertaining to business chats would be shared with Facebook while personal messages, group chats, contacts, and locations have remained end-to-end encrypted; and Facebook or any third party would not have access to user content in any way. WhatsApp then pushed in-app notifications directing users towards blog posts that provided clarification of the policy in simple language and managed to rebuild some trust without necessarily unraveling core data-sharing provisions (Wulandari, et al., 2024).

ALIGNMENT WITH GLOBAL DATA PROTECTION REGULATIONS

GDPR Requirements vs. WhatsApp Practices

The table below illustrates the key provisions of General Data Protection Regulation (GDPR) and their correspondence to WhatsApp practices. The table highlights compliance and areas of concern:

Table 4. GDPR Requirements vs. WhatsApp Practices

GDPR Provision	WhatsApp's Practice	Compliance Status	Citations
Article 6(1)(a) – Lawfulness of processing: Consent	WhatsApp requires user consent for data processing. However, concerns have been raised about the clarity and granularity of this consent, especially regarding data sharing with Facebook.	Partially compliant; transparency issues noted.	(Hakobyan, et al., 2025; Kim, et al., 2025).
Article 12 – Transparent information, communication, and modalities	In 2021, the Irish Data Protection Commission (DPC) fined WhatsApp €225 million for failing to provide transparent information about data processing, particularly concerning information shared with Facebook companies.	Non-compliant; remedial actions required.	(Lim, & Yu, 2025; G'sell, 2025).
Article 5(1)(c) – Data minimization	WhatsApp collects metadata such as device information and usage patterns. Critics argue that some of this data collection exceeds what is necessary for service provision.	Partially compliant; data minimization practices under scrutiny.	(Hakobyan, et al., 2025; Gonzales, 2025).
Chapter V (Articles 44–50) – Transfers of personal data to third countries	WhatsApp transfers data between the EU and the U.S., relying on Standard Contractual Clauses (SCCs) following the invalidation of the Privacy Shield framework.	Compliant with current SCCs; ongoing legal challenges may affect future compliance.	(Althubiti & Sevegnani, 2025; Bhattacharyya & Adhikary, 2025).

DPDP Requirements vs. WhatsApp Practices

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

Table 5. DPDP Requirements vs. WhatsApp Practices

DPDP Provision	WhatsApp's Practice	Compliance Status	Source
§ 6(1) Consent: "free, specific, informed, unconditional, unambiguous"	In January 2021, WhatsApp forced users to accept its entire updated Privacy Policy via a full-screen banner (single "Accept" button) without granular opt-outs for individual processing operations.	Partial: Consent obtained, but not granular	meity.gov.in, moengage.com
§ 13 Data-Principal Rights: access, correction, erasure, portability	Offers "Request Account Info" report (settings & metadata only) but no direct in-app correction, no export of chat history, and deleted-account backups remain in cloud unless user manually purges	Partial: Access enabled; correction/portability limited	whatsapp.com
§ 9 & Rules 10 (Children's Data): verifiable parental consent	Parents/guardians page allows self-attested inquiries and consent, but lacks robust age-verification or independent identity checks	Partial: Mechanism exists but not verifiable	meity.gov & whatsapp.com
§ 17 & Rules 7 (Breach Notification): notify DPBI within 72 hrs	No individual breach notices to users or DPBI; relies on aggregated Meta transparency reports with no user-level alerts	Non-compliant	lexology.com
Rules 6 (Security Safeguards): encryption, access limits, record-keeping	Strong in-transit E2EE; optional encrypted backups; default Google Drive/iCloud backups unencrypted; extensive metadata logging; no independent audit reports	Partial: Safeguards in transit; backup & logging gaps	ey.com
§ 16 (Cross-Border Transfers): only to notified jurisdictions	Processes user data globally (Meta servers in U.S., Ireland, Singapore); relies on SCCs rather than India-only whitelist	Non-compliant	meity.gov
§ 6(7) Consent Manager: neutral third-party consent management	No external consent manager; consent flows solely through WhatsApp's own UI, without a "manager" role	Non-compliant	prsindia.org
§ 18 Establish DPBI: create Data Protection Board of India	DPBI not yet constituted; no published decisions or guidance under DPDP Act	Pending	meity.gov.in
§ 37 Penalties & Blocking Orders: fines up to ₹250 Cr; repeat breaches → block	No DPDP-Act penalties or blocking orders to date; WhatsApp has instead faced CCI penalties under competition law for its 2021 policy in India.	Pending	reuters.com

The Digital Personal Data Protection Act, 2023 (DPDP Act) and Draft DPDP Rules, 2025 together represent the first comprehensive data-privacy legislation for the world's largest democracy. Notable innovations include a formalized Consent Manager, fixed timelines for breach notifications, and platforms faced with an order to cease operations under Section 37. However, pending the final Rules of the Draft DPDP Act, along with the constitution of the Data

Protection Board of India, most of these requirements remain on paper (Pawar, 2025).WhatsApp practice is partially in sync: end-to-end encryption and user-controlled account-info reporting reflect a strong "security by design" and can be considered ally in the case against the platforms, while the consent banner with one-size-fits-all provisions, with the default unencrypted backup and global data flow systems, may not be in consonance with Indian mandates. The lack of individual breach notifications and granular opt-outs renders the platform vulnerable to significant gaps against the requirements in the DPDP Act (Barat, 2024).

The Ministry of Electronics & IT (MeitY) has put out for public consultation the Draft Rules from carrying out fine-tuning of the operational aspects since the DPDP Act came into existence on 11 August 2023 (3 January 2025-18 February 2025). So far, there have been no penalties under the DPDP, but DPBI can fine up to ₹250 Cr and issue blocking orders for repeat offenders. At the same time, MeitY has also signaled its intention to notify cross-border transfers under which data fiduciaries will not be able to transfer data to jurisdictions other than those approved by the government under Rule X of the final Rules. Other than under the DPDP framework, Indian agencies have used existing IT-Act powers to look into WhatsApp's data-sharing practices. The Justice B.N. Srikrishna Committee proposed stronger oversight, while MeitY has been pressed by parliamentary questions to disclose transparency concerning the 2021 update to the Privacy Policy. While no formal investigations under the DPDP Act against WhatsApp are public at the moment, the swift movement of the government into Rule-making clearly signals to platforms that they must comply quickly or incur hitherto unseen levels of fines and operational restrictions (meity.gov.in).

So far, WhatsApp has taken up end-to-end encryption technology, which robustly protects messages in transit, but only partially complies with the Digital Personal Data Protection Act, 2023 (DPDP Act) as well as upcoming Rules. Broad rather than granular flows of consent occupy the place of relatively few limited user-rights implementations as well as breach-notification practices found wanting on statutory provisions. Now, though, Indian authorities-from MeitY to the CCI-have begun to initiate both new and old tools to beef up data privacy safeguards while making platforms accountable for their actions. DPDP Act § 6(1) states: "free, specific, informed, unambiguous" consent with individual opt-ins for each processing purpose. In January 2021, all users were compelled by WhatsApp to accept wholesale policy changes via a singe "Accept" button-and without allowing selective opt-outs-for individual data uses. Under DPDP § 13, users must be in a position to access, correct, erase or port their personal data. Although WhatsApp offers a "Request Account Info" report exporting certain metadata, there is no possibility in the app to edit profile information or export full chat histories (reuters.com). In addition, deleted-account backups often remain in Google Drive or iCloud until manually purged by the user. These limitations contravene both the spirit and letter of the Act's rights provisions.

In compliance with DPDP § 17 and Rule 7, the data fiduciaries are obliged to notify the Data Protection Board of India (DPBI) and affected principals regarding any personal data breaches within 72 hours. WhatsApp, however, adopts a policy of not sending individualized alerts to users or informing the yet-to-be-set-up DPBI and instead places reliance upon Meta's reports, which disclose information in aggregate concerning breaches. Draft Digital Personal Data Protection Rules, 2025 for public comments from January 3, 2025, to February 18, 2025, later extended to March 5, invited suggestions from stakeholders to improve breach-notification timelines, cross-border transfer limits, and the Consent Manager mechanism (ey.com) in contradistinction with the operationalization of the DPDP Act. In a second part of the antitrust intervention, the Delhi Commission imposed a penalty of ₹213.14 Crore on Meta in November 2024 for abusing its dominant position through WhatsApp's "forced consent" model and barred the collection of data under this guise with other Meta entities over the next five years. This intervention in the antitrust law dealt with the same consent-granularity issues codified later under DPDP § 6(1). While the Data Protection Board of India—a body set up under DPDP § 18—has yet to be formally established, its creation is imminent, providing an adjudicatory authority with the power to impose penalties of up to ₹250 Crore and block the operation of non-compliant platforms by § 37. Once India finalizes its Rules and operationalizes the DPBI, WhatsApp and other digital services will be obliged to fast-track granular consent, extend user-rights tools, and put in place rapid breach-notification systems in order to avoid incurring penalties under both the antitrust regime and the DPDP Act.(lexology.com).

Compliance with Other Frameworks (CCPA, LGPD, etc.)

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

The following table compares major global data protection laws in terms of the year they were enacted, the primary user rights they have conferred, and Worx' status in terms of compliance:

Table 6. Law regarding WhatsApp

Law	Country /Region	Year Enacted	Core User Rights	WhatsApp Compliance	Citations
General Data Protection Regulation (GDPR)	European Union	2018	Right to access, rectify, erase data; data portability; object to processing; restrict processing; not be subject to automated decision-making.	Partially compliant; fined €225 million in 2021 for transparency violations.	(Dimova, et al., 2023).
California Consumer Privacy Act (CCPA)	USA (California)	2018	Right to know about personal data collected; delete personal data; opt-out of sale of personal data; non-discrimination for exercising rights.	Generally compliant; however, integration with Facebook's advertising ecosystem raises concerns.	(Tran, et. al., 2024).
Lei Geral de Proteção de Dados (LGPD)	Brazil	2018	Right to confirm existence of processing; access data; correct incomplete/inaccurate data; anonymize, block, or delete unnecessary data; data portability; revoke consent.	Updated policies to align with LGPD requirements; ongoing monitoring by Brazil's National Data Protection Authority (ANPD).	(ALMADA, 2023)
Digital Personal Data Protection Act (DPDPA)	India	2023	Right to access, correction, erasure, grievance redressal; appoint another to exercise rights on data principal's behalf in event of death/incapacity.	Under scrutiny for alleged violations of Section 72 of the IT Act and 2011 Rules; compliance status under evaluation.	Singh & Singh, 2025).
Data Protection Act 2018	United Kingdom	2018	Mirrors GDPR rights; includes provisions specific to the UK context post-Brexit.	Compliance status similar to GDPR; subject to UK Information Commissioner's Office oversight.	(Morris, et al., 2021).
California Privacy Rights Act (CPRA)	USA (California)	2020	Expands CCPA rights; right to correct inaccurate personal data; limit use and disclosure of sensitive personal information; strengthens enforcement mechanisms.	Compliance status under evaluation; must adhere to enhanced requirements effective from January 1, 2023.	King & Stephan, (2021).
Protection of Personal Information Act (PoPIA)	South Africa	2013	Right to be informed; access personal information; correct or delete personal information; object to processing; not be subject to automated decision-making.	Compliance status under evaluation; must ensure adherence to PoPIA provisions enforced from July 1, 2020.	(de Waal, 2022).
Personal Information	China	2021	Right to know and decide on processing; restrict or refuse	Compliance status under evaluation;	(Calzada, 2022).

Protection Law (PIPL)			processing; access and copy personal information; correct and delete personal information; data portability.	must navigate stringent cross-border data transfer restrictions.	
Personal Data Protection Act (PDPA)	Singapore	2012	Right to access and correct personal data; withdraw consent for data collection, use, or disclosure.	Compliance status under evaluation; must ensure adherence to PDPA provisions and updates.	(Chik, 2013).
Personal Data Protection Bill	Australia	Pending	Proposed rights include access, correction, deletion, and data portability; strengthening consent requirements; and enhancing enforcement powers.	Compliance status to be determined upon enactment; proactive measures recommended.	(Paterson & McDonagh, 2018).

Regulatory Enforcement and Sanctions

- **Ireland's DPC Fines (e.g., €225 million, 2021):** The Data Protection Authority of Ireland decided against WhatsApp in September 2021, for which it imposed a hefty penalty of £225 million, ostensibly for violating GDPR in terms of transparency with its users about data processing. The decision was adjudged after lengthy investigations which had started in 2018 and has had various influences by other European data protection authorities (Daigle, & Khan, 2022).
- **Ongoing Investigations and Corrective Orders:** According to WhatsApp, the DPC's decision is being appealed because the penalty is excessive. This matter has been referred to the CJEU, which will likely render a judgment next calendar year. WhatsApp was also instructed to take corrective measures to align its data processing with the requirements of the GDPR (G'sell, 2025).

IMPACT OF DIGITAL SURVEILLANCE ON WHATSAPP USERS

Transparency Reports and Benchmark Data

WhatsApp falls under the precinct of Meta Platforms, and in recent times, the app has come up under the harsh glare of scrutiny especially by the user data-sharing practices with governments. For instance, in the first half of 2022, India happened to file up to 55,497 requests for user data, which included 51,602 under legal processes and 3,895 emergency requests. About 66.59 percent of those requests have been complied with by Meta, by releasing some user data in response to the requests. Such volumes of requests underscore how dependent governments now are on such digital platforms for surveillance and law enforcement. While Meta continues to profess its commitment to and practice user privacy, this heavy compliance rate raises questions regarding how much user information is ultimately protected from government overreach (Kira, 2025).

User-Level Impact Metrics

a) **Account Takeovers and Phishing Campaigns:** Whatsapp adopted preventive measures against all forms of scams and has terminated accounts involved in such activities. In October 2022, WhatsApp banned over 2.3 million accounts in India. Out of these, 811,000 bans were enforced proactively, before any user complaint was registered. Such proactive bans show WhatsApp's commitment to finding and preventing all types of harmful activities taking place on the platform. Still, the sheer volume of banned accounts serves as an indicator to substantiate that there are long-standing problems in the area of prevention against malicious activities and ensuring security for users (Angafor, 2025).

b) **Spyware Exploit Cases: Pegasus and Paragon:** Among the most widely renowned spyware targeting WhatsApp users, one can name Pegasus and Paragon.

- **Pegasus (NSO Group):** In 2019, Pegasus spyware was used to infiltrate about 1,400 persons worldwide, including journalists and activists. In 2024, a U.S. judge ruled that NSO Group was responsible for these hacks (Lubin, 2025).
- **Paragon Solutions:** In December 2024, WhatsApp disrupted a spyware campaign by Paragon Solutions targeting around 90 journalists and civil society members. The spyware exploited a zero-click vulnerability, which WhatsApp has since patched (CHUAH, et al., 2025).

These incidents underscore the vulnerabilities in digital communication platforms and the lengths to which malicious actors will go to surveil and suppress dissenting voices.

Case Studies & Statistics

The following table consolidates key data points related to digital surveillance impacts on WhatsApp users:

Table 7. Case studies

Category	Details	Source
Government Data Requests (India)	In the first half of 2022, India submitted 55,497 requests for user data to Meta platforms, including WhatsApp. This included 51,602 legal process requests and 3,895 emergency disclosure requests. Meta complied with 66.59% of these requests, providing some user data in response.	Newslaundry
Account Bans (India, Oct 2022)	Between October 1 and 31, 2022, WhatsApp banned over 2.3 million accounts in India for violating platform policies. Of these, approximately 811,000 accounts were proactively banned before any user reports were filed.	Business Standard
Pegasus Spyware Attack (2019)	In 2019, Pegasus spyware, developed by NSO Group, was used to target approximately 1,400 individuals globally, including journalists and activists. A U.S. judge ruled NSO Group liable for these hacks in 2024, allowing the case to proceed to trial on the question of damages.	Reuters
Paragon Spyware Campaign (2024)	In December 2024, WhatsApp disrupted a spyware campaign by Paragon Solutions targeting around 90 journalists and civil society members. The spyware exploited a zero-click vulnerability, which WhatsApp has since patched.	The Verge

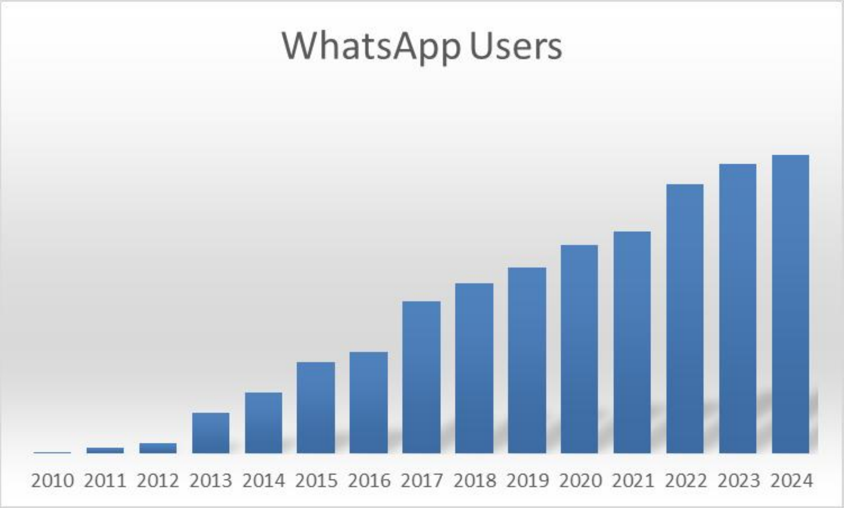


Figure 13: WhatsApp Monthly Active Users (Worldwide)

Source: https://backlinko.com/whatsapp-users

Table 8. WhatsApp Monthly Active Users (Worldwide)

Year	**WhatsApp Users (approx..)**
2010	10,000,000
2011	50,000,000
2012	100,000,000
2013	400,000,000
2014	600,000,000
2015	900,000,000
2016	1,000,000,000
2017	1,500,000,000
2018	1,680,000,000
2019	1,830,000,000
2020	2,060,000,000
2021	2,190,000,000
2022	2,660,000,000
2023	2,860,000,000
2024	2,950,000,000
2025*	3,500,000,000 (est.)

Source: https://backlinko.com/whatsapp-users

STRATEGIES FOR MITIGATING CYBERSECURITY RISKS

Technical Safeguards

- **End-to-end Encrypted Cloud Backups**: Adopting end-to-end encryption for cloud-based backups ensures that data remains unintelligible from the point of origin through storage and retrieval. Encryption keys should be generated and stored exclusively under organizational control, preventing any third-party access—even by the cloud provider. Versioning mechanisms can preserve historical file states without sacrificing confidentiality, while automated integrity checks validate successful backups and flag any unauthorized modifications (Putri, 2025).
- **Two-Step Verification & Security Code Checks:** Requiring two distinct authentication factors—something possessed (a hardware token or mobile authenticator app) plus something known (a PIN or password)—dramatically reduces the likelihood of unauthorized account access. Time-based -Time Passwords (TOTP) and FIDO2-compliant security keys elevate resistance against phishing and replay attacks. Adaptive authentication policies may further assess risk signals (geolocation, device fingerprinting, anomalous behavior) and prompt additional verification when a session deviates from established baselines (Holtgrave, et al., 2025).

Organizational and User Education Measures

- **Metadata Minimization Whitepapers:** Disseminating detailed whitepapers on metadata minimization empowers developers, administrators, and end users to understand how hidden data elements—timestamps, revision histories, embedded sensor logs—can inadvertently reveal sensitive information. Clear guidelines should outline automated stripping tools for document formats, recommended default settings for data-sanitization libraries, and retention schedules that balance forensic traceability with privacy preservation. Periodic reviews of these whitepapers reinforce evolving best practices as new file types and collaboration platforms emerge (Esterhuyse, et al., 2025).

- **Anti-Phishing/Malware Training & Best-Practice Guides:** Conducting realistic phishing simulations coupled with interactive workshops cultivates a security-first mindset among all personnel. Training modules should cover social-engineering indicators, payload delivery techniques, and incident-reporting workflows. Publishing concise best-practice guides—covering safe link-clicking behaviors, attachment handling, patch-management awareness, and secure configuration checklists—provides quick-reference materials that support ongoing vigilance. Measuring click-through and reporting rates identify knowledge gaps and informs the frequency and focus of follow-up sessions (Ashawa, 2021).

Enterprise-Grade Configurations and Monitoring:

Centralizing security configurations and monitoring under an enterprise-grade framework enables continuous visibility and rapid response. A hardened baseline configuration—aligned with industry benchmarks such as the CIS Controls—defines secure defaults for operating systems, network devices, and application platforms. Real-time log aggregation into a Security Information and Event Management (SIEM) system facilitates the correlation of disparate events, while automated alerting triggers predefined playbooks for containment and remediation. Incorporating User and Entity Behavior Analytics (UEBA) uncovers subtle deviations from normal patterns, surfacing insider threats or compromised credentials with minimal delay. Regular audits of configuration drift, vulnerability scans, and red-team exercises validate the resilience of these controls over time (Joseph, 2023).

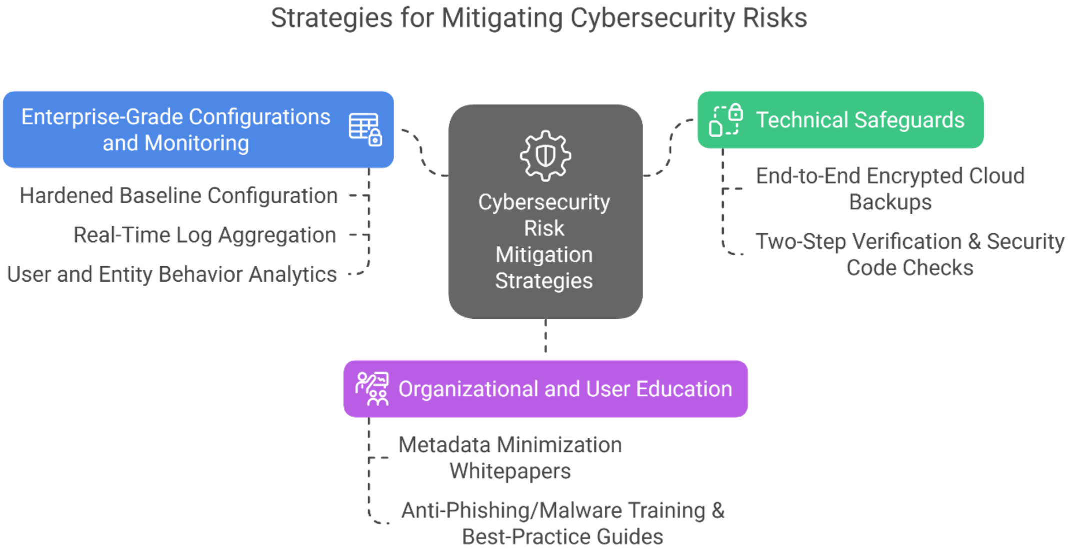

Strategies for Mitigating Cybersecurity Risks
Enterprise-Grade Configurations and Monitoring
Hardened Baseline Configuration
Real-Time Log Aggregation
User and Entity Behavior Analytics
Cybersecurity Risk Mitigation Strategies
Technical Safeguards
End-to-End Encrypted Cloud Backups
Two-Step Verification & Security Code Checks
Organizational and User Education
Metadata Minimization Whitepapers
Anti-Phishing/Malware Training & Best-Practice Guides

Figure 14: Strategies for mitigating cybersecurity Risks

Source: Self-prepared by author

Table 9. Evolution of WhatsApp's Privacy Policies & Policy Recommendations

Stage & Date	Privacy Policy Highlights	User Impact & Concerns	Key Policy Recommendations	Citations
2009–2015	• Account tied to phone number • Minimal data shared; basic metadata (timestamps,	• Simple sign-up, but opaque around what metadata was stored or how long it was retained.	• Publish clear data-retention schedules • Introduce a metadata-minimization audit	(Sulistiani, 2025).

	contacts) collected for service			
April 2016	• Default end-to-end encryption for all chats and calls (Signal Protocol) • "Read receipts" configurable	• Strong confidentiality guarantees for message contents; • Some confusion over metadata still being visible	• Offer transparency on metadata collection • Provide a "metadata view" dashboard for users	(Dimova, et al., 2023).
Jan 2021	• Update to share certain business-chat data with Facebook (e.g. transaction data, usage)	• Massive user backlash over forced consent; • Migration to rival platforms (Signal, Telegram)	• Implement granular opt-in/opt-out controls per data category • Publish plain-language summaries	(Aldalbahi & Albesher, 2023).
Late 2023	• Launched Privacy Hub with FAQs and transparency reports; • Expanded controls over disappearing messages	• Better education on controls, though many users are still unaware of settings	• Regularly update the Privacy Hub with real-world examples • Proactive in-app nudges about settings	
Ongoing/Future	• Periodic "trust" reports; • Growth of business APIs and catalog data sharing	• Users must balance the convenience of business features against privacy; default settings often remain "on"	• Adopt "privacy by default" (opt-in defaults) • External audits of compliance; publish findings	(Isman & El Mrassni, 2023).

CONCLUSION

In-depth and elaborate analyses of WhatsApp privacy policies vis-à-vis digital surveillance, data protection by users within the environment, and finally, its cybersecurity features were conducted in this study. It drew critical examinations of issues such as policy shifts, user responses, and also compliance or noncompliance with international data protection frameworks such as GDPR, CCPA, and LGPD. From here, it highlighted advances with persistent gaps in WhatsApp's approach toward user privacy. End-to-end encryption, while WhatsApp employs, protects message content; however, there is still a considerable amount of holes, such as in metadata collection, unencrypted cloud backups, and exposure to spyware attacks. This most relevant and current change in the privacy policy--the requirement to share user data with parent company Meta (formerly Facebook)--created a buzz amongst users and led to a massive backlash and an upsurge in opting for privacy-centered alternatives like Signal and Telegram. In this regard, it pinpoints that trust, transparency, and self-ownership are three critical factors that would define the future of digital communication platforms. With the DPDP Act, 2023 and the DPDP Rules, 2025 introduced by India to strengthen data protection, platforms such as WhatsApp must guarantee granular consent, breach notifications, and data principal rights. Compliance pressure will be enhanced through regulatory enforcement of the forthcoming Data Protection Board. Businesses should exert privacy by design and bring their practices into line with the evolving legal framework in India.

The examination further validated the only partial adherence of WhatsApp to worldwide privacy laws. For example, failures in transparency have confronted it with regulatory actions, including a €225 million fine from Ireland's Data Protection Commission (Daigle, et. al., 2022). Whereas WhatsApp's efforts at clarifying its data policy—through FAQs and public outreach—have been commendable, they have been insufficient to lift public scrutiny, especially outside of the European Union, where data protections are comparatively weak. It further studied how surveillance capitalism and the privacy paradox explain user behavior amid growing surveillance: Users will often accept invasive terms for lesser perceived trade-offs or, in well-publicized cases, due to sheer ignorance of what their rights are. There is a need for substantial education regarding privacy issues led by civil societies. In the meantime, governments continue to demand backdoors into encrypted services in the name of national security—ones that pose a direct threat to the integrity of end-to-end encryption and user rights.

From the standpoint of cybersecurity, the rise of phishing attacks, malware campaigns, and zero-click spyware like Pegasus and Paragon shows that technical loopholes can create havoc even on encrypted platforms. When threats like those outlined above intertwine with ambiguities in policies, they expose a complex relationship between corporate interests, regulatory responses, and user expectations. The study proposes several improvements to data sharing, including enhanced user controls, default encryption for messaging and backups in the cloud, transparent privacy policies, greater regulatory oversight, international harmonization of data protection standards, and continuous public campaigns to educate users on privacy settings and emerging threats. The study also recommends that a zero-trust security model be considered for greatest future implementation to mitigate the risk of internal and external breaches and calls on WhatsApp to release periodic independently audited transparency and trust reports.

Future research must assess the impact of policy changes on long-term user behavior, study how AI can assist in real-time privacy enforcement, and evaluate how effectively regional data protection laws are working in practice to hold corporations accountable. The future of the world is dependent on technology, but still, attention must be placed on user privacy and cybersecurity resilience as public policy development advances. The evolution of WhatsApp privacy policies reflects the larger struggle over user privacy as they become monetized by the company and their communications are being watched by government agencies. A multidimensional approach-including ethical design, good regulation, active engagement with users, and constant vigilance against improvement implementation is needed to balance all these competing interests of privacy, profit, and supervision. Only this history can provide digital privacy in an age of surveillance capitalism.

REFRENCES

[1] Adorjan, M., & Ricciardelli, R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. Canadian review of sociology = Revue canadienne de sociologie, 56 1, 8-29 . https://doi.org/10.1111/cars.12227.

[2] Aldalbahi, S. S., & Albesher, A. S. (2023). Young Saudis' evaluations and perceptions of privacy in digital communities: the case of WhatsApp and telegram. Sustainability, 15(14), 11286.

[3] Alić, M., & Sopić, L. (2023, May). Privacy Paradox and Generation Z. In 2023 46th MIPRO ICT and Electronics Convention (MIPRO) (pp. 1532-1537). IEEE.

[4] ALMADA, M., & MARANHÃO, J. (2023). Contribuiçoes e limites da lei geral de proteçao de dados para a regulaçao da inteligência artificial no brasil. Revista direito público, 20, 385-413.

[5] Althubiti, E., & Sevegnani, M. (2025). Modeling Privacy Compliance in Cross-border Data Transfers with Bigraphs. arXiv preprint arXiv:2503.20464.

[6] Angafor, G. N. (2025). Social media security: the impact of AI-generated Whatsapp scams on the security and privacy of Whatsapp community groups.

[7] Ashawa, M. A. (2021). The detection and prevention of Malware attacks on android mobile through the application of artificial intelligence techniques (Doctoral dissertation).

[8] Barat, D. (2024). An Overview of India's New Data Protection Law. J. on Governance, 7, 11.

[9] Bawake, H., Cholke, S., Dhole, A., Jadhav, A., & Bhise, P. (2023). E2EE Web Messaging Application Using Cryptography Techniques. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2023.50633.

[10] Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. Computers & Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2021.107546.

[11] Bhat, M., Bajaj, V., & Kumar, S. (2020). The crime vanishes: Mob lynching, hate crime, and police discretion in India. Jindal Global Law Review, 11, 33 - 59. https://doi.org/10.1007/s41020-020-00115-4.

[12] Bhattacharyya, P., & Adhikary, S. (2025). Shifting Work Paradigms: Legal Perspectives on India's Digital Revolution.

[13] Bucci, R., Kirk, D., & Sampson, R. (2022). Visualizing How Race, Support for Black Lives Matter, and Gun Ownership Shape Views of the U.S. Capitol Insurrection of January 6, 2021. Socius, 8. https://doi.org/10.1177/23780231221110124.

[14] Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). Smart Cities, 5(3), 1129-1150.

[15] Chai, S., Nicholson, B., Scapens, R., & Yang, C. (2023). Digital Platforms, Surveillance and Process of Demoralization. Journal of Information Technology. https://doi.org/10.1177/02683962231208215.

[16] Challacombe, D., & Patrick, C. (2022). The January 6th insurrection at the U.S. capitol: What the TRAP-18 can tell us about the participants.. Journal of Threat Assessment and Management. https://doi.org/10.1037/tam0000194.

[17] Chamorro-Atalaya, O., Aguilar, M., Candia-Quispe, W., Roman-Gonzalez, A., Cruz-Telada, Y., Suarez-Bazalar, R., & Arévalo-Tuesta, J. (2023). Voice Analytics for the Identification of University Student Satisfaction, from WhatsApp Audio Messaging. Int. J. Emerg. Technol. Learn., 18, 219-227. https://doi.org/10.3991/ijet.v18i21.39073.

[18] Chen, C., Wei, L., Zhang, L., Peng, Y., & Ning, J. (2022). DeepGuard: Backdoor Attack Detection and Identification Schemes in Privacy-Preserving Deep Neural Networks. Security and Communication Networks. https://doi.org/10.1155/2022/2985308.

[19] Chik, W. B. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. Computer Law & Security Review, 29(5), 554-575.

[20] CHUAH, K., DELI, R. M., & CH'NG, L. C. (2025). Gen Z and Group Work: How Communication Styles Affect Free-Riding Behaviours. Gen, 41(1), 423-437.

[21] Cooray, M., Rajuhan, I., & Adnan, W. (2023). Industry approaches in handling online exploitation of children: A comparative study of the policy, guidelines and best practices in Malaysia, Singapore and Australia. Cogent Social Sciences, 9. https://doi.org/10.1080/23311886.2023.2241713.

[22] Crystal-Ornelas, R., Varadharajan, C., O'Ryan, D., Beilsmith, K., Bond-Lamberty, B., Boye, K., ... & Agarwal, D. A. (2022). Enabling FAIR data in Earth and environmental science with community-centric (meta) data reporting formats. Scientific data, 9(1), 700.

[23] Daigle, B., & Khan, M. (2022). The changing tides of data protection regulation and enforcement in Europe. Office of Industries, US International Trade Commission.

[24] de Waal, P. J. (2022). The protection of personal information act (POPIA) and the promotion of access to information act (PAIA): It is time to take note. Current Allergy & Clinical Immunology, 35(4), 232-236.

[25] Desolda, G., Ferro, L., Marrella, A., Catarci, T., & Costabile, M. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys (CSUR), 54, 1 - 35. https://doi.org/10.1145/3469886.

[26] Dimova, Y., Kode, M., Kalantari, S., Wuyts, K., Joosen, W., & Mühlberg, J. T. (2023, November). From privacy policies to privacy threats: a case study in policy-based threat modeling. In Proceedings of the 22nd Workshop on Privacy in the Electronic Society (pp. 17-29).

[27] Durrant, T., Lilly, A., & Tingay, P. (2022). WhatsApp in government. How ministers and officials should use messaging apps–and how they shouldn't. London: Institute for Government.

[28] Edo, O., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering. https://doi.org/10.46338/ijetae0722_15.

[29] Endeley, R. (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. Journal of Information Security, 09, 95-99. https://doi.org/10.4236/JIS.2018.91008.

[30] Endeley, R. E. (2019). End-to-end Encryption, Backdoors, and Privacy. Capitol Technology University.

[31] Erfina, A., Hidayat, R., Rafli, R., Rizaldi, R., Maulana, R., & Falentino, T. (2023). Analyzing Code Injection Attacks on Applications of Android Devices and Emulator. 2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED), 1-6. https://doi.org/10.1109/ICCED60214.2023.10425065.

[32] Esterhuyse, C. A., Müller, T., & van Binsbergen, L. T. (2025). JustAct+: Justified and Accountable Actions in Policy-Regulated, Multi-Domain Data Processing. arXiv preprint arXiv:2502.00138.

[33] Gonzales, W. D. W. (2025). Predicting language choice in a digital medium: A computational approach to analyzing WhatsApp code-switching in Hong Kong. International Journal of Bilingualism, 13670069251325036.

[34] G'sell, F. (2025). Digital Authoritarianism: from state control to algorithmic despotism. Available at SSRN 5117399.

[35] Haddad, A., Habaebi, M., Elsheikh, E., Islam, M., Zabidi, S., & Suliman, F. (2024). E2EE enhanced patient-centric blockchain-based system for EHR management. PLOS ONE, 19. https://doi.org/10.1371/journal.pone.0301371.

[36] Hakobyan, O., Hillmann, P. J., Martin, F., Böttinger, E., & Drimalla, H. (2025). Development and evaluation of Dona, a privacy-preserving donation platform for messaging data from WhatsApp, Facebook, and Instagram. Behavior Research Methods, 57(3), 1-17.

[37] Hari, A., & Abdulla, M. S. (2023). WhatsApp as a Superapp: Chatbots, Business API and the challenges ahead (No. 583).

[38] Hashmi, S., George, N., Saqib, E., Ali, F., Siddique, N., Kashif, S., Ali, S., Bajwa, N., & Javed, M. (2023). Training Users to Recognize Persuasion Techniques in Vishing Calls. Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3544549.3585823.

[39] Henkoglu, T. (2022). Privacy Perception of Social Network Platforms Regarding the Information Policies: Evaluation of User Information Behavior. Celal Bayar Üniversitesi Sosyal Bilimler Dergisi. https://doi.org/10.18026/cbayarsos.1055166.

[40] Holtgrave, C., Nouwens, M., & Klokmose, C. (2022). Caught in the Network: The Impact of WhatsApp's 2021 Privacy Policy Update on Users' Messaging App Ecosystems. Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3491102.3502032.

[41] Holtgrave, J. U., Klivan, S., Marky, K., & Fahl, S. (2025). A Qualitative Study of Adoption Barriers and Challenges for Passwordless Authentication in German Public Administrations.

[42] Hunn, C., Spiranovic, C., Prichard, J., & Gelb, K. (2020). Why internet users' perceptions of viewing child exploitation material matter for prevention policies. Australian & New Zealand Journal of Criminology, 53, 174 - 193. https://doi.org/10.1177/0004865820903794.

[43] Isman, A., & El Mrassni, H. (2023). ANALYZING THE DIFFUSION OF WHATSAPP AS AN INNOVATIVE COMMUNICATION TOOL IN MOROCCO: FACTORS AFFECTING USER ADOPTION, BEHAVIORS, AND ATTITUDES. The Online Journal of New Horizons in Education-October, 13(4).

[44] Jena, K. (2023). Zero-Trust Security Models Overview. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit2390578.

[45] Joseph, A. (2023). A Holistic Framework for Unifying Data Security and Management in Modern Enterprises. International Journal of Social and Business Sciences, 17(10), 602-609.

[46] Kalogeropoulos, A., & Rossini, P. (2025). Unraveling WhatsApp group dynamics to understand the threat of misinformation in messaging apps. New Media & Society, 27(3), 1625-1650.

[47] Kalpana, C., Rushikesh, N., & Srikanth, A. (2023). Backdoor Entry to a Windows Computer. International Journal of Advanced Research in Science, Communication and Technology. https://doi.org/10.48175/ijarsct-9616.

[48] Khrishkevich, T. (2022). Right-wing Extremist Organizations of Modern Germany: Attempts to Revise History as a Threat to Social Cohesion. Metamorphoses of history. https://doi.org/10.37490/mh2022235.

[49] Kim, G., Hur, U., Kang, S., & Kim, J. (2025). Analyzing the Web and UWP versions of WhatsApp for digital forensics. Forensic Science International: Digital Investigation, 52, 301861.

[50] King, J., & Stephan, A. (2021). Regulating privacy dark patterns in practice-drawing inspiration from California Privacy Rights Act.

[51] Kira, B. (2025). Inter-agency coordination and digital platform regulation: lessons from the Whatsapp case in Brazil. International Review of Law, Computers & Technology, 39(1), 6-29.

[52] Koczur, S. (2022). Pirates of Privacy: How Companies Profit Off Your Data by Using Capital Surveillance Methods in Criminal Prosecution. Journal of Science Policy & Governance. https://doi.org/10.38126/jspg210106.

[53] Li, T. (2024). Analysis of Personal Privacy Risks and Protection Countermeasures under the Privacy Paradox Dimension. Transactions on Social Science, Education and Humanities Research. https://doi.org/10.62051/tsnrh462.

[54] Lim, D., & Yu, P. K. (2025). The antitrust–copyright interface in the age of generative artificial intelligence. Emory Law Journal, 74, 24-87.

[55] Limoncelli, T. (2023). Improvement on End-to-End Encryption May Lead to Silent Revolution. Queue, 21, 10 - 13. https://doi.org/10.1145/3590144.

[56] Liu, Y., Tantithamthavorn, C., Li, L., & Liu, Y. (2021). Deep Learning for Android Malware Defenses: A Systematic Literature Review. ACM Computing Surveys, 55, 1 - 36. https://doi.org/10.1145/3544968.

[57] Lubin, A. (2025). Unpacking WhatsApp's Legal Triumph Over NSO Group. Lawfare.

[58] Maglaras, L., Ayres, N., Moschoyiannis, S., & Tassiulas, L. (2022). The end of Eavesdropping Attacks through the Use of Advanced End to End Encryption Mechanisms. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1-2. https://doi.org/10.1109/infocomwkshps54753.2022.9798072.

[59] Manji, K., Hanefeld, J., Vearey, J., Walls, H., & De Gruchy, T. (2021). Using WhatsApp messenger for health systems research: a scoping review of available literature. Health Policy and Planning, 36, 774 - 789. https://doi.org/10.1093/heapol/czab024.

[60] Morris, C., Scott, R. E., & Mars, M. (2021). WhatsApp in clinical practice—the challenges of record keeping and storage. A scoping review. International journal of environmental research and public health, 18(24), 13426.

[61] Nene, S. T. A. (2017). Legislation, Policy, and Regulation in the Post-telecommunication Era: The Role of OTT Service's (WhatsApp) Consumption and Sense-making in the Everyday Lives of Black-middle Class Employees of Parliament of the Republic of South Africa (Doctoral dissertation, University of KwaZulu-Natal, Pietermaritzburg).

[62] Nicol, S., Harris, D., Kebbell, M., & Ogilvie, J. (2021). Online child sexual exploitation material: A comparison from police data on men charged with child sexual exploitation material exclusively and men charged with contact child sexual abuse exclusively. Sexual Offending: Theory, Research, and Prevention. https://doi.org/10.5964/sotrap.4301.

[63] Nojeim, G., & Maheshwari, N. (2020). Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth. Indian Journal of Law and Technology. https://doi.org/10.55496/hgck9762.

[64] Olaniyi, O., & Omubo, D. (2023). WhatsApp Data Policy, Data Security, and Users' Vulnerability. International Journal of Innovative Research and Development. https://doi.org/10.24940/ijird/2023/v12/i4/apr23021.

[65] Olaniyi, O., & Omubo, D. (2023). WhatsApp Data Policy, Data Security, and Users' Vulnerability. International Journal of Innovative Research and Development. https://doi.org/10.24940/ijird/2023/v12/i4/apr23021.

[66] Paterson, M., & McDonagh, M. (2018). Data protection in an era of big data: The challenges posed by big personal data. Monash University Law Review, 44(1), 1-31.

[67] PAWAR, S. (2025) How BDSLCCI can Help SMEs to Achieve Data Protection Compliance, Such as EU GDPR and the DPDP Act of India.

[68] Perry, S., & Roda, C. (2017). User Privacy in a World of Digital Surveillance. , 63-93. https://doi.org/10.1057/978-1-137-58805-0_3.

[69] Putri, A. (2025). Multi-Cloud Strategies for Managing Big Data Workflows and AI Applications in Decentralized Government Systems. Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks, 9(1), 1-11.

[70] Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. ERA Forum, 21, 429 - 447. https://doi.org/10.1007/s12027-020-00625-7.

[71] Rancati, L., & de Ghellinck, E. (2019). The intersection between antitrust and data protection. Lessons from the Facebook/Whatsapp merger and the Bundeskartellamt's decision on Facebook's terms and conditions. Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain, 2019-2021.

[72] Reis, J., Melo, P., Garimella, K., & Benevenuto, F. (2020). Can WhatsApp benefit from debunked fact-checked stories to reduce misinformation? Harvard Kennedy School Misinformation Review. https://doi.org/10.37016/mr-2020-035.

[73] Rösler, P., Mainka, C., & Schwenk, J. (2018, April). More is less: On the end-to-end security of group chats in Signal, WhatsApp, and three. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 415-429). IEEE.

[74] Rossini, P., & Kalogeropoulos, A. (2023). Don't talk to strangers? The role of network composition, WhatsApp groups, and partisanship in explaining beliefs in misinformation about COVID-19 in Brazil. Journal of Information Technology & Politics. https://doi.org/10.1080/19331681.2023.2234902.

[75] Sahoo, N. R., Beria, G. P., & Bhattacharyya, P. (2024). IndicCONAN: A Multilingual Dataset for Combating Hate Speech in Indian Context. Proceedings of the AAAI Conference on Artificial Intelligence, 38(20), 22313-22321. https://doi.org/10.1609/aaai.v38i20.30237

[76] Santos, M., & Faure, A. (2018). Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. Social Media + Society, 4. https://doi.org/10.1177/2056305118795876.

[77] SATYANARAYANA, D. P. (2021) PRIVACY AS A FUNDAMENTAL RIGHT: THE SUPREME COURT'S PERSPECTIVE IN INDIA. INNOVATIVE RECENT TRENDS IN, 150.

[78] Shen, Y. (2021). End-to-End Encrypted Messaging Based on PGP with Forward Secrecy. Journal of Physics: Conference Series, 1873. https://doi.org/10.1088/1742-6596/1873/1/012031.

[79] Singh, R. K., & Singh, V. (2025). Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023. Journal of Indian Academy of Forensic Medicine, 09710973251328785.

[80] Soares, F., Recuero, R., Volcan, T., Fagundes, G., & Sodré, G. (2021). Research note: Bolsonaro's firehose: How Covid-19 disinformation on WhatsApp was used to fight a government political crisis in Brazil. . https://doi.org/10.37016/MR-2020-54.

[81] Sudjayanti, S., & Hamdani, D. (2024). Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method. Brilliance: Research of Artificial Intelligence. https://doi.org/10.47709/brilliance.v4i1.3800.

[82] Sulistiani, I. (2025). COMMUNICATION DYNAMICS THROUGH INSTANT MESSAGING APPLICATIONS: A LITERATURE ANALYSIS OF THE TELEGRAM AND WHATSAPP PLATFORMS.

[83] Sur, S. (2021). Digital Privacy: Case Study Analysis on Whatsapp Privacy Policy Changes. International Journal of Applied Science and Engineering. https://doi.org/10.30954/2322-0465.2.2021.4.

[84] Talwar, A., Chaudhary, A., & Kumar, A. (2022, October). Encryption Policies of Social Media Apps and Its Effect on User's Privacy. In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-4). IEEE.

[85] Tiwari, R. (2024). Digital privacy and data protection in the age of surveillance. International Journal of Law, Justice, and Jurisprudence. https://doi.org/10.22271/2790-0673.2024.v4.i2c.139.

[86] Tran, V., Mehrotra, A., Chetty, M., Feamster, N., Frankenreiter, J., & Strahilevitz, L. (2024). Measuring Compliance with the California Consumer Privacy Act Over Space and Time. Proceedings of the CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3613904.3642597.

[87] Trautman, L. J. (2019). Governance of the Facebook Privacy Crisis. Pitt. J. Tech. L. & Pol'y, 20, 43.

[88] Vijay, J., & Singh, S. S. (2023). KS Puttaswamy Judgment After-effects: Moving Towards Transformative Constitutionalism. DME Journal of Law, 4(01), 8-14.

[89] Wulandari, S., Rahma, A., & Bakthawar, P. (2024). Connotation and Myth: Language Expression of Gen Z through WhatsApp Emoticon. Wicara: Jurnal Sastra, Bahasa, dan Budaya. https://doi.org/10.14710/wjsbb.2024.23294.

[90] Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. Organization Theory, 3(3), 26317877221129290.