PRIMUS PARTNERS®

Quote by Arun Moral, Managing Director, Primus Partners

Published in Awadh 360

What's Up with WhatsApp?

Authored By Prateek Shukla

Read on: https://awadh360.com/articles/business/whats-up-with-whatsapp

Article Content:

When Zoho founder Sridhar Vembu recently called out Meta's data practices as fundamentally at odds with user privacy, he wasn't just making another tech industry gripe. He was articulating what cybersecurity experts have been warning about for years: businesses using WhatsApp for critical operations are essentially handing over their most sensitive information to a company whose business model depends on data extraction.

"It is naive to assume these companies will put user privacy first," Vembu stated bluntly, referring to Meta and other advertising-driven platforms. The timing of his comments -- coinciding with Elon Musk's explosive lawsuit against Meta over WhatsApp's data practices -- has thrust an uncomfortable question into the spotlight: Why are Indian businesses, from startups to established corporations, conducting mission-critical operations on a platform they neither own nor control?

The Illusion of Privacy

Step into any Indian office, and you might see WhatsApp at the heart of it all: employee coordination groups buzzing with updates, client communications flying back and forth, vendor negotiations sealed in hasty threads, financial details hashed out in real time, product launches coordinated down to the last detail. Even HR matters -- performance reviews, salary discussions -- are increasingly confined to those deceptively innocuous green chat bubbles.

The scale of this reliance is staggering. India boasts over 535 million WhatsApp users, making it the platform's largest market worldwide. An estimated 70–80% of Indian small and medium businesses lean on WhatsApp Business for customer engagement. For countless enterprises, entire departments operate through these groups, freely sharing strategic plans and customer databases with barely a nod to data security.

Yet most users miss the bigger picture: every message, document, and voice note routed through WhatsApp funnels straight to Meta's servers. Sure, the company touts end-to-end encryption for messages in transit, but the metadata -- who's messaging whom, at what hour, how often, which groups they're in, whose contacts they're syncing -- remains fully exposed to Meta.

And the kicker? Those cloud backups that users flip on by default? They're not end-to-end encrypted at all. "WhatsApp’s biggest risk for businesses isn’t message surveillance, it’s the false sense of operational privacy it creates. While conversations may be encrypted in transit, the surrounding data, relationships, frequency, group structures, backups, and business behaviour, creates a rich intelligence layer. Indian companies have effectively turned a consumer messaging app into critical infrastructure, without governance, ownership, or audit control. That’s not a technology failure; it’s a strategic blind spot," said Haritima Amrawat, Founder & CEO, Éclat d’or, a UK-based law firm management consultancy.

Dependency Runs Deep

For millions of Indian businesses, WhatsApp isn't just a tool -- it's the backbone of daily operations. Take manufacturing firms: They orchestrate entire supply chains via the app, from suppliers firing off quotations to purchase orders zipped over as PDF attachments. Quality control snags get dissected in group chats laced with on-site photos, and payment confirmations wrap up with a quick voice note. All of it -- the pricing strategies, vendor ties, production timelines -- sits exposed on Meta's global servers.

Startups aren't faring much better. Founding teams debate their next moves in WhatsApp huddles; investor pitch decks get forwarded in a flash; customer feedback trickles in through WhatsApp Business channels. HR groups dissect salary structures, while cap tables,

revenue breakdowns, and scraps of competitive intel zip through the ether -- all on a platform bankrolled by targeted ads.

“From a legal and compliance standpoint, the widespread use of WhatsApp for business operations raises serious cross-border data exposure concerns. Messages may feel private, but businesses often overlook where data is stored, how backups are handled, and which jurisdictions may have access to associated information. For companies operating across India, the Middle East, and Europe, this creates regulatory ambiguity—particularly around confidentiality, client privilege, and data localisation expectations. Informal communication channels blur accountability and weaken audit trails. As regulatory scrutiny tightens globally, businesses must reassess whether convenience-driven platforms are suitable for sensitive legal, commercial, and financial communications,” said Ajmal Khan Nadakkal, Managing Partner, ABS Partners Legal Consultants (UAE).

What's at Risk?

The above-mentioned aren't idle worries -- they're baked-in vulnerabilities, layered and insidious:

Business Espionage: Discussions on competitor intel, pricing maneuvers, product roadmaps, or M&A whispers over WhatsApp could lay bare to Meta, opening the door to breaches. Remember Meta's 2021 data spill, which exposed phone numbers and personal details for 530 million users?

Employee Privacy: HR chats delving into performance red flags, salary haggling, firing protocols, or health disclosures risk trampling employee rights under India's tightening data protection rules.

Client Confidentiality: For lawyers, accountants, and consultants, shuttling client files via WhatsApp could shatter privilege duties. In finance or healthcare, that's not just sloppy -- it's a regulatory infraction.

Intellectual Property: Snapshots of product blueprints, code fragments, algorithms, or trade secrets flung into chats forge weak links in IP defenses, often unnoticed until disaster strikes.

Regulatory Exposure: India's Digital Personal Data Protection Act (DPDPA) is live now, holding data-handling businesses to strict fiduciary standards. Learning on WhatsApp for staff or client info without ironclad safeguards? That could draw fines up to ₹250 crores.

“WhatsApp’s shift into a super-app intensifies convenience, but also concentrates consent, metadata and behavioural data. Under India’s DPDP framework, the core challenge is not encryption of messages, but whether consent remains granular,revocable and enforceable across the full data lifecycle,” said Arun Moral, Managing Director, Primus Partners.

The Meta Business Model Problem

Boil it down, and the rift is simple: incentives don't align. Meta thrives on data -- every connection mapped, every pattern traced, every interest inferred fuels a $134 billion ad machine in 2023 alone. WhatsApp wears the "private messaging" badge,

but it's stitched into a fabric woven from surveillance capitalism.

Vembu's jab lands right there: "These companies' business models are fundamentally based on collecting and monetizing user data. Expecting them to prioritize privacy is expecting them to act against their own economic interests."

Meta insists WhatsApp stands apart, fortified by encryption and stingy on data swaps. Still, its privacy fine print admits sharing user tidbits across the family of companies "to improve your experiences and their services." Business profiles? They're an open book --profiles, customer chats, transaction logs all fair game for Meta's gaze.

Alternatives Exist, But Adoption Lags

Here's the twist—viable paths out are right there, including homegrown ones. But they're gathering dust.

Tools like Slack, Microsoft Teams, and Zoho Cliq deliver the goods: admin lockdFowns, local data hosting, message archiving, and forensic trails. These aren't bells and whistles; they're table stakes for any outfit serious about its comms.

Then there are the locals: Nandbox, Troop Messenger, Kaveri. Built for India, compliant with its laws, data parked domestically, no bowing to Silicon Valley overlords. So why the cold shoulder? WhatsApp's gravitational pull -- network effects on steroids.

Everyone's plugged in already. Uprooting means herding not just your team, but clients, suppliers, the whole web of partners. The upfront hassle feels crushing.

That's the trap, though -- the very stickiness that spells trouble. Firms opt for the easy now over the secure tomorrow.

The Path Forward: What Indian Businesses Must Do

Ditching WhatsApp cold turkey? Not always practical -- it's still gold for outward-facing banter or promo blasts. The real pivot is carving it out of the core: internal ops, high stakes talks. Here’s what businesses can do: -

Conduct a data audit: Trace every thread in your WhatsApp groups. Flag the red flags -- finances, personnel files, client intel, IP blueprints, boardroom blueprints. If a leak would sting, it's off-limits there.

Establish clear policies: Draft iron rules on WhatsApp dos and don'ts. Plenty of firms' police social media but let chats run wild, even as they're woven deeper into the workday.

Migrate critical functions: Shift team syncs, project tracking, and delicate deliberations to locked-down enterprise setups. WhatsApp can linger for the low-risk bits; it's about matching tools to threats.

Educate employees: Most folks conflate transit encryption with true lockdown. They skip how backups betray you or metadata maps your world.