

WhatsApp Usernames And The Hard Question Of Identity Online

Nikhil Narendran

A mistaken identity on a social network can lead to misinformation, and a counterpublic infrastructure, including factchecking, can be built to counter it. A mistaken identity on a messaging platform can lead to a digital arrest scam, investment fraud, real-life or online abuse, including in private spaces, or a sophisticated impersonation of a government officer. That distinction matters a lot in India



Summary

- WhatsApp's new username feature is seen as a privacy win globally but a fraud risk in India.
- The Indian government sought clarity from Meta before the feature's rollout.
- The episode shows digital identity regulation is becoming more contextual and localised.

When WhatsApp announced that users would soon be able to communicate via usernames rather than phone numbers, the global reaction was overwhelmingly positive. The feature was widely celebrated as an overdue privacy enhancement. After all, why should someone have to disclose their personal mobile number just to chat?

Privacy advocates welcomed it as a step towards data minimisation and privacy by design. WhatsApp, many argued, was finally catching up with platforms such as Telegram and Signal.

India's reaction could not have been more different. The Indian government reportedly asked Meta to explain the implications before rolling it out. The discussion quickly shifted from privacy to fraud, impersonation and cybercrime. Digital rights groups criticised the government's intervention as regulatory overreach, while many argued that the government's concerns were entirely legitimate given the scale of financial fraud on messaging platforms.

The same feature was celebrated as a privacy safeguard in one jurisdiction while being viewed as a public safety concern in another. This is perhaps another reminder that the era of a single unified internet is already over.

The Internet has spent three decades trying to answer a deceptively simple question of how to manage identity online. The first generation of the Internet encountered this problem through domain names. Every website required a unique identity, even though language itself was rarely unique. Domain name registries, trademark law, and dispute-resolution mechanisms gradually emerged because someone had to decide who could legitimately claim a particular identity online. That debate is still unresolved, and there are several pending Indian cases that deal with website squatting.

Social media inherited the same dilemma. Some platforms encouraged pseudonyms, whereas others insisted on real names, with neither model being entirely satisfactory. Pseudonymity expanded privacy and free expression while simultaneously making impersonation and abuse easier. Real-name policies improved accountability but raised concerns about surveillance, exclusion, and privacy.

Messaging platforms now represent the next stage in that evolution. Unlike social media, messaging platforms are not designed primarily for publishing content. They are designed to allow one individual to establish direct communication with another. That seemingly small distinction fundamentally changes the nature of the risks.

A mistaken identity on a social network can lead to misinformation, and a counterpublic infrastructure, including factchecking, can be built to counter it. A mistaken identity on a messaging platform can lead to a digital arrest scam, investment fraud, real-life or online abuse, including in private spaces, or a sophisticated impersonation of a government officer.

That distinction matters a lot in India.

India has undergone one of the world's fastest digital transformations. Hundreds of millions of citizens have entered the formal digital economy through smartphones, UPI and Aadhaar. Organised fraud networks have

adapted just as quickly with cross-border call centres, fake investment platforms, government impersonation scams and financial fraud often specifically targeting elderly citizens and first-generation digital users.

Identity performs a different function in India's digital ecosystem than in many Western jurisdictions, where the dominant concern is limiting the disclosure of personal information. In India, privacy remains important, but so does trust in digital interactions. How easily a bad actor can establish credibility with a potential victim now matters as much as how much a user reveals.

This is also the regulatory backdrop against which the username feature lands. The Department of Telecommunications has already directed messaging apps built on mobile number infrastructure, WhatsApp included, to maintain checks and balances such as continuous SIM binding and automatic logout of web sessions, treating them as telecommunication identifier user entities. The regulator had just finished tightening the phone number as the anchor of accountability when a feature arrived proposing to push it into the background.

Seen in this light, the Government's engagement with WhatsApp is fair and consistent. The law already treats WhatsApp as infrastructure, and rightly so. It carries everything from **family conversations to commerce** for hundreds of millions of people, and when a foundational feature of such infrastructure changes, the trust ecosystem built around it can erode quickly and quietly.

Notice also what the Government did not do. There is no ban here. There is a consultation before a feature is rolled out. That is probably the direction technology regulation should take, because once the cat is out of the bag, it is nearly impossible to put it back in. If social media regulation has taught us anything, it is that the right questions asked at the right time could have stopped some harms from arriving at all.

For multinational technology companies, the broader lesson is that digital regulation is becoming contextual. A feature designed to solve one problem may create another in a different jurisdiction, and product design can no longer assume that the conditions prevailing in California, Brussels or London exist in Bengaluru, Lucknow or Guwahati.

The deeper shift is that public identity on communications networks, once anchored to a telecom-issued mobile number, is increasingly a platform-managed username. Platforms are becoming custodians of digital identity, deciding who receives a username, which identities deserve protection, how impersonation is addressed and how disputes are resolved. Privacy gains of that scale need governance of equal seriousness, particularly where organised digital fraud is a systemic challenge.

India's response to WhatsApp's username feature may age well. It reflects an early recognition that digital identity cannot be governed identically across every society, and that regulation will depend less on universal product design and more on how technology interacts with local institutions, risks and social realities.

(Views expressed are personal.)

