WHATSAPP USERNAMES AND THE FUTURE OF DIGITAL IDENTITY

AUTHORED BY:
MR. VEDANT SARAF
PARTNER

SKR & ASSOCIATES

CHAPTER 1: INTRODUCTION

WhatsApp's proposed introduction of usernames represents more than a routine product enhancement. It signals a fundamental shift in how digital identity is created, presented and trusted on one of the world's largest communication platforms. Since its launch, WhatsApp's identity model has been built around a simple premise: every account is linked to a mobile telephone number. While a telephone number does not, by itself, establish the identity of an individual, it has historically provided a degree of external assurance. In India, this assurance is strengthened by the fact that mobile numbers operate within a regulated telecom ecosystem and are ordinarily linked to subscribers through KYC-based SIM issuance requirements. The proposed username feature changes this model. Users will be able to communicate through self-selected alphanumeric identifiers without disclosing their underlying mobile numbers. From a privacy perspective, this is an important and welcomed development. Reducing the routine exposure of telephone numbers can address several longstanding concerns, including spam, unsolicited communication, harassment, data scraping and certain forms of online abuse. However, the implications of this transition extend beyond privacy.

The existing WhatsApp ecosystem derives a measure of trust from the fact that every account is anchored to a unique telephone number. A username-based system moves that trust towards a platform-controlled identifier whose authenticity depends substantially on the rules, safeguards and enforcement mechanisms established by Meta. This shift raises an important regulatory question. As digital platforms increasingly determine how individuals establish and verify identity online, should the law continue to address risks only after harm occurs, or should platforms also bear responsibility for identifying and mitigating foreseeable risks at the stage when digital identity systems are designed?

The concern is not that usernames are inherently problematic. Digital platforms across the world have successfully operated username-based systems for years. Nor should privacy-enhancing measures be discouraged merely because they create new regulatory considerations. The issue is whether a change that fundamentally alters the way users assess trust online requires corresponding safeguards to preserve authenticity and prevent misuse. This question assumes particular significance in India. The country's rapidly expanding digital ecosystem has resulted in increasing reliance on online communication for financial services, commerce and interactions with public institutions. At the same time, cyber fraud has become increasingly dependent on social engineering techniques rather than sophisticated technical attacks. Fraudsters often succeed not by obtaining unauthorised access to systems, but by convincing individuals that they are interacting with a trusted person or institution.

Investment scams, phishing campaigns, impersonation of banks and government authorities, and so-called "digital arrest" frauds operate on precisely this vulnerability: the victim's misplaced confidence in the identity of the person communicating with them. In such an environment, the manner in which digital identity is presented and authenticated becomes a matter of consumer protection and platform governance, not merely product design. Meta has indicated that usernames will be accompanied by safeguards intended to reduce impersonation risks, including restrictions on certain identifiers and measures to detect abusive behaviour. These steps are relevant and necessary. However, they remain primarily matters of internal platform policy. Indian law does not currently prescribe detailed obligations requiring intermediaries to undertake structured assessments of identity-related risks before implementing significant changes to their authentication architecture.

This article argues that WhatsApp's proposed username feature highlights a broader gap in India's digital regulatory framework. Existing laws, including the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules**"), provides important remedies against misuse, fraud and impersonation. However, these frameworks largely operate after harm has occurred. They do not impose meaningful design-stage obligations requiring platforms to evaluate and mitigate foreseeable risks arising from changes to digital identity systems. As platforms increasingly replace externally verifiable identifiers with platform-controlled identities, the legal question is no longer limited to how data is collected or how unlawful content is removed. It extends to a more fundamental issue: how trust itself is designed in the digital environment.

CHAPTER 2: THE SHIFT FROM EXTERNALLY ANCHORED IDENTITY TO PLATFORM-CONTROLLED IDENTITY

The significance of WhatsApp's proposed username feature lies not merely in the introduction of a new method of identification, but in the underlying change in how trust is established between users. A mobile telephone number has traditionally served as a basic identity anchor in digital communication. It is not a perfect verification mechanism. A number can be transferred, misused or obtained fraudulently. Nevertheless, it possesses certain characteristics that distinguish it from a purely platform-generated identifier. A telephone number exists within an external regulatory framework. It is issued by telecom service providers, linked to subscriber information and subject to regulatory requirements relating to customer identification. The credibility of the identifier therefore does not arise solely from the platform using it; it is supported by a broader institutional framework.

A username operates differently. A username is created and governed entirely within the platform ecosystem. Its availability, uniqueness, visibility, verification and enforcement depend on decisions made by the intermediary. The platform effectively becomes responsible for determining how much confidence users should place in that identifier. This does not mean that username-based systems cannot be trusted. Many digital platforms have built sophisticated mechanisms around usernames, including verification badges, reputation systems and abuse detection tools. However, the transition places greater responsibility on platforms because the safeguards that support trust become internal rather than externally anchored.

The practical consequences of this shift are significant. Digital impersonation rarely succeeds through exact duplication. Fraudsters typically rely on creating sufficient similarity to appear legitimate. A username that differs by a single character, punctuation mark or minor spelling variation may be enough to mislead users, particularly in environments where communication occurs quickly and individuals make trust decisions based on familiarity rather than detailed verification.

For example, a user may reasonably assume that a message from a username closely resembling that of a bank, business executive, government authority or known contact is genuine. The deception does not depend upon the fraudulent account being identical; it depends upon the possibility of confusion. This risk becomes particularly important in India because digital fraud has increasingly moved towards identity-based manipulation. The growth of online banking, digital payments and platform-driven commerce has created a greater dependence on digital identifiers as proxies for trust. The regulatory challenge is therefore not limited to preventing misuse after impersonation occurs. It concerns whether platforms should incorporate safeguards at the stage when identity systems are designed.

A username system that protects privacy but permits easy impersonation creates one set of risks. A system that exposes personal telephone numbers indefinitely in the name of authenticity creates another. The objective should not be to choose between privacy and trust, but to develop identity systems that advance both. The responsibility of platforms in achieving this balance is likely to become increasingly important. As digital intermediaries assume a greater role in facilitating communication, commerce and financial activity, decisions relating to identity architecture can no longer be viewed solely as internal product choices. They have broader implications for consumer protection, cybersecurity and confidence in the digital ecosystem.

CHAPTER 3: THE DOCTRINAL GAP: WHY EXISTING LAW STOPS AT REACTIVE ENFORCEMENT

The debate surrounding WhatsApp's proposed username feature highlights a broader limitation in India's digital regulatory framework. The issue is not that Indian law fails to recognise impersonation, fraud or misuse of digital platforms. Rather, the existing framework largely addresses these risks after they have materialised, without imposing corresponding obligations on platforms to anticipate and mitigate foreseeable risks at the stage when digital systems are designed.

This distinction is increasingly important. Digital platforms today do not merely provide communication infrastructure. They actively shape the environment in which users assess identity, authenticity and trust. Decisions relating to account creation, identity verification, username allocation, discoverability and reporting mechanisms influence the likelihood of fraud and impersonation. These are no longer purely technical or commercial decisions; they have direct consequences for users and the broader digital ecosystem. Yet Indian law continues to approach these issues primarily through a reactive enforcement model.

The DPDP Act provides an important framework for regulating the processing of personal data. It establishes obligations relating to notice, consent, purpose limitation, security safeguards and the rights of Data Principals. However, the statute is principally concerned with how personal data is collected, processed and protected. It does not seek to regulate the architecture through which digital identities are created or presented. Consequently, risks arising from misleading usernames do not fit neatly within the DPDP Act's regulatory framework. A fraudulent username may cause significant harm without necessarily involving unlawful processing of another individual's personal data. The harm arises from deception, confusion and misplaced reliance rather than from the misuse of personal information in the traditional sense. This is not a limitation of the DPDP Act. Rather, it reflects the fact that privacy legislation and identity governance address different regulatory concerns.

The IT Act similarly provides important remedies but operates primarily after wrongful conduct has occurred. Sections 66C and 66D address identity theft and cheating by personation using computer resources. These provisions remain critical tools for enforcement against digital fraud. The IT Rules also impose obligations on intermediaries to take reasonable measures against certain forms of unlawful activity, including impersonation. Intermediaries are required to establish mechanisms for receiving complaints and responding to specified categories of unlawful content.

However, these provisions are fundamentally reactive. They assume that impersonation or misuse has already taken place and prescribe obligations relating to response, removal or enforcement. They do not require platforms to undertake structured assessments before introducing changes that may materially affect how users establish trust online.

For example, the existing framework does not prescribe minimum standards regarding:

- assessment of impersonation risks arising from new identity features;
- reservation of usernames associated with public figures, businesses or government institutions;
- mechanisms for identifying confusingly similar identifiers;
- transparency regarding platform verification processes; or
- user warnings where identity ambiguity creates heightened risks.

The Bharatiya Nyaya Sanhita, 2023 follows a similar approach. It criminalises fraudulent conduct once the elements of an offence are established, but it does not regulate the technological systems that may facilitate such conduct. This is consistent with the traditional role of criminal law, which is designed to attribute responsibility after wrongful conduct rather than prescribe technical standards for product development.

Taken together, these statutes reveal a broader regulatory gap. Indian digital regulation currently separates privacy, intermediary responsibility and criminal liability into distinct legal categories. Each regime serves an important purpose. However, there remains limited regulation of the space between product design and legal enforcement, the stage at which foreseeable risks may be identified and addressed before users suffer harm.

This gap becomes increasingly significant as digital platforms assume greater control over identity systems. Historically, digital identity was often anchored to external institutions: telecom operators, banks, government-issued identifiers or other regulated entities. Increasingly, however, identity is becoming platform-defined. The credibility of an individual's digital presence depends less on external verification and more on the internal rules established by private technology companies. That transition does not necessarily require heavy-handed regulation. Requiring prior government approval for every product innovation would be impractical and undesirable.

However, there is a legitimate regulatory question regarding whether platforms of significant scale should undertake proportionate assessments of foreseeable risks when making changes that affect digital identity and user trust. The regulatory conversation must therefore move beyond the question of whether platforms have complied with existing obligations after harm occurs. It must also consider whether platforms have taken reasonable steps to prevent foreseeable harm when designing systems that millions of users rely upon.

CHAPTER 4: PRIVACY AND AUTHENTICITY NEED NOT BE COMPETING OBJECTIVES

The discussion around WhatsApp's username feature also highlights a common tension in digital regulation: the perceived trade-off between privacy and accountability. Privacy advocates may view the removal of mandatory phone number visibility as an important step towards protecting users. That view is justified. For many individuals, particularly those participating in public groups, professional communities or interactions with unknown users, limiting exposure of personal telephone numbers can significantly reduce unwanted communication, harassment and misuse.

However, privacy alone cannot be the only measure of a successful digital identity system. Privacy and authenticity serve different but complementary purposes. Privacy protects information about an individual. Authenticity enables users to form reasonable confidence regarding the identity of the person or institution with whom they are interacting. A system that protects privacy but undermines confidence in identity creates

its own risks. Conversely, a system that maximises transparency by exposing personal identifiers may impose unnecessary privacy costs. The regulatory objective should therefore not be to prioritise one over the other. It should be to design systems where privacy protection and identity assurance operate together.

The WhatsApp username proposal illustrates this challenge. Removing the requirement to disclose telephone numbers may reduce one category of harm while potentially increasing another. The question is whether additional safeguards can preserve the privacy benefits without weakening user confidence. Possible approaches could include stronger verification mechanisms for high-risk accounts, enhanced protections for businesses and public institutions, improved detection of confusingly similar usernames, greater transparency around identity indicators, and user education regarding the limitations of digital identifiers.

The law currently provides limited guidance on achieving this balance. The DPDP Act focuses primarily on responsible processing of personal data. The intermediary framework focuses largely on obligations relating to unlawful content and complaints. Neither framework directly addresses how platforms should balance privacy-enhancing design choices against risks arising from reduced identity visibility. This reflects a broader characteristic of India's digital regulatory approach. Legislative attention has historically focused on questions of data collection, processing, cybersecurity and intermediary liability. The design of digital identity systems has largely remained within the discretion of technology platforms.

That approach may require reconsideration. As platforms increasingly facilitate financial transactions, professional interactions and public communication, identity design becomes a matter of broader societal importance. The question is not whether governments should dictate product architecture. Rather, it is whether large digital intermediaries should be expected to apply reasonable safeguards when their design decisions directly influence user trust and exposure to fraud.

The future of digital regulation will likely require moving beyond a narrow distinction between privacy regulation and cybercrime enforcement. Digital trust depends on both the protection of personal information and the ability of users to make informed judgments about who they are communicating with. A privacy-enhancing technology should therefore not be assessed solely by how effectively it conceals personal information. It should also be evaluated on whether it preserves confidence, accountability and safety within the digital ecosystem.

CHAPTER 5: CONCLUSION: MOVING TOWARDS TRUST-BY-DESIGN REGULATION

WhatsApp's proposed username feature should not be viewed merely as a change to how users exchange messages. It represents a broader evolution in the manner in which digital identity is created and trusted online. For years, digital platforms have relied upon identifiers that were at least partially connected to external systems of verification. Telephone numbers, email addresses, bank accounts and government-issued identifiers provided varying degrees of assurance because they were linked to institutions operating outside the platform itself. The next phase of digital platforms is likely to be different. As privacy considerations become increasingly important, platforms will continue moving towards identity systems that minimise exposure of personal information. This transition is desirable. Users should not be required to permanently disclose sensitive personal identifiers merely to participate in digital communication.

However, the movement towards platform-controlled identities also carries corresponding responsibilities. The existing Indian regulatory framework provides important protections once digital harm occurs. Criminal law addresses fraud and impersonation, intermediary regulations establish obligations relating to unlawful content

and user complaints, and the DPDP Act provides a comprehensive framework governing the processing and protection of personal data. Each of these frameworks serves an important purpose.

The question raised by WhatsApp's username feature is whether these frameworks are sufficient when the risk itself originates from the design of a digital system. A platform that changes the way millions of users establish trust inevitably influences the conditions under which fraud and impersonation may occur. This does not mean that every product decision should require regulatory approval. Such an approach would be neither practical nor desirable. Excessive regulation may discourage innovation, delay privacy-enhancing developments and create unnecessary barriers for technology platforms.

The alternative, however, cannot be complete reliance on voluntary safeguards. A balanced approach would recognise the importance of proportionate, technology-neutral obligations requiring large digital platforms to consider foreseeable risks when introducing significant changes to identity systems.

Such obligations could include:

- conducting internal risk assessments before deploying identity-related features;
- implementing safeguards against confusingly similar usernames, particularly for public institutions, businesses and high-risk entities;
- maintaining transparent processes for verification and impersonation reporting;
- providing appropriate warnings where identity ambiguity may create heightened risks; and
- publishing sufficient information regarding the safeguards adopted to protect users.

These measures would not require regulators to determine how platforms should build their products. Instead, they would establish a minimum expectation that platforms consider user safety as part of product design. This approach would align with a broader global movement towards "safety by design" and "privacy by design" principles, where responsibility is placed not only on responding to harm but also on reducing foreseeable risks before they materialise. For India, this conversation is particularly relevant. The country is experiencing rapid digitisation across banking, commerce, governance and communication. As more aspects of daily life move online, confidence in digital identity will become increasingly important. A regulatory framework that focuses only on post-harm remedies may not adequately address risks arising from the architecture of digital systems themselves.

The debate surrounding WhatsApp usernames therefore raises a question that extends far beyond one platform feature: When private technology platforms increasingly determine how individuals establish identity and trust online, should the law recognise certain responsibilities in the design of those systems? The answer is unlikely to lie in choosing between innovation and regulation, or between privacy and accountability. The challenge is to develop a framework that enables technological progress while ensuring that trust remains a deliberate outcome of digital design rather than an assumption. As digital identities become increasingly platform-defined, the design of those identities will become inseparable from questions of consumer protection, cybersecurity and legal responsibility. Digital trust cannot be created only after fraud occurs. It must be designed into the systems that shape how individuals interact online.

ABOUT THE AUTHOR

Mr. Vedant Saraf

Vedant is a Partner and heads the corporate law department at SKR & Associates. Vedant routinely advises Indian and international banks, financial institutions, sponsors, investment funds, and corporates on a broad spectrum of domestic and cross-border transactions. His practice focuses on syndicated and bilateral lending, structured finance, project finance, refinancing, external commercial borrowings, security structuring, corporate structuring and re-structuring, commercial contracts, and regulatory advisory. Vedant has advised clients across diverse sectors, including renewable energy, infrastructure, real estate, and financial services. He can be reached at **vedant@skradvocates.com**