



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

FROM PHONE NUMBERS TO USERNAMES: WHATSAPP'S NEW FEATURE AND THE EVOLVING LANDSCAPE OF DIGITAL PRIVACY IN INDIA

~ *Bhumika Singh*

INTRODUCTION

For nearly fifteen years, a WhatsApp account has been inseparable from a phone number. Recently, Meta has introduced a new feature which aims to replace phone numbers with usernames as digital identifiers, also changing how users connect on the platform.¹ Although it's still in the pre-released phase, it has found itself surrounded by a debate over its impact on digital privacy as the Indian government has reportedly issued a notice to Meta to pause the roll-out.²

Traditionally, users were identified with phone numbers, which is also considered a digital identifier across multiple platforms, making it privacy-sensitive. Therefore, the introduction of usernames marks a significant shift towards privacy-oriented digital platforms. While the feature appears to reflect the principles of data minimisation and informational privacy under the 2002 OECD Privacy guidelines, it also raises concerns over anonymity, accountability, and regulatory oversight.³

PHONE NUMBERS AS DIGITAL IDENTIFIERS

¹ Abhishek Dey, *Why India Is Concerned About WhatsApp Usernames*, BBC News (July 2, 2026), <https://www.bbc.com/news/articles/ckg8e0n9l41o>.

² *Why India Is Concerned About WhatsApp Usernames and What It Could Mean for Other Countries*, Channel News Asia, <https://www.channelnewsasia.com/asia/why-india-concerned-about-whatsapp-usernames-and-what-it-could-mean-other-countries-6238151>.

³ Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2002), <https://doi.org/10.1787/9789264196391-en>.

Initially, phone numbers were used as a tool for contact in the physical world, not specifically intended to serve as identifiers or authentication tools. However, they have gradually evolved to become user identifiers as it has become difficult to even form digital accounts without providing a phone number.⁴

Phone numbers are continuously used for Multi-Factor Authentication (MFA) and account recovery, because of which they also act as a key that links profile data across digital platforms and devices. Since users provide the same phone numbers across platforms, companies can also use data aggregation to extract all the information about that individual to form a comprehensive “digital person.”⁵ This digital person reveals a detailed portrait consisting of data of an individual across platforms that was initially never intended to be shared.

This unwanted exposure creates what scholars call “context collapse,” where numbers shared in one context can be used to expose information in unexpected ways.⁶ For example, a single phone number can be used by researchers or malicious actors to quickly uncover a person’s home address, family members, criminal history, and more. This can also occur due to phone number recycling and security vulnerabilities like SIM swapping attacks.

Since phone numbers have become persistent digital identifiers, minimising their disclosure becomes a major privacy concern.

LEGAL FRAMEWORK

Before any law was passed, these privacy issues were initially handled through constitutional interpretation during the *K.S. Puttaswamy v. Union of India* case.⁷ It recognised the right to privacy as a fundamental right enshrined in Article 21 of the Indian Constitution. Alongside the right, the digital platforms were regulated through the IT Act (2000)⁸, but no specific act was passed in regards to the right to privacy until 2023.

Later, the Digital Personal Data Protection (DPDP) Act was passed in 2023.⁹ It is the first comprehensive legislation for the protection of data and privacy in India. It ensures that the

⁴ Allison McDonald et al., *The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling*, in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021).

⁵ Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 507 (2006).

⁶ McDonald et al., *supra* note 4.

⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁸ Information Technology Act, 2000 (India).

⁹ Digital Personal Data Protection Act, No. 22 of 2023 (India).

personal data is handled lawfully. Under this act personal data is defined as “any data about an individual who is identifiable by or in relation to such data.” It calls the individual “Data Principal” to whom personal data relates to, and the entity (government or private) handling such data is referred to as the “Data Fiduciary.”¹⁰

Here, Meta is the Data Fiduciary, while WhatsApp users are Data Principals. Where a Data Fiduciary fails to comply with obligations of processing and protecting the personal data under the Act, the data fiduciary may be held accountable. The DPDP Act mandates the data fiduciary to implement “appropriate technical and organizational measures” to prevent any breaches or misuse, failing which the penalties can go up to Rupees 250 crore.¹¹ Meta argues that it complies with these mandates through several “layers of defence,” consisting of reserved usernames, restricted contact and search, username key, and contextual information provided to the users.¹²

For now, the new feature seems to be consistent with broader data protection principles, particularly reducing unnecessary exposure of personal identifiers by replacing the phone numbers with usernames.

PRIVACY, PSEUDONYMITY, AND REGULATORY CHALLENGES

As discussed above, phone numbers have traditionally been known as digital identifiers. Since these would be hidden if the feature is rolled out, the usernames would replace it. However, usernames do not mean complete anonymity; rather, it is as Moore describes “pseudonymity.”¹³ Users will no longer reveal their phone number as identifiers to everybody they interact with. However, WhatsApp would still have the phone number details through registration data and backend systems. This has the potential to strengthen privacy while ensuring accountability.

Nevertheless, it has still posed a few governance challenges. This has prompted the government of India to reportedly issue a notice¹⁴ to pause the roll out citing concerns over future cybercrime possibilities as the fraudsters can choose the usernames resembling that of officials, banks, celebrities, or government institutions to scam people. The pseudonymity

¹⁰ Digital Personal Data Protection Act, No. 22 of 2023, §§ 2(i), 2(j), 2(t) (India).

¹¹ Digital Personal Data Protection Act, No. 22 of 2023, § 8(4), sched. (India).

¹² Dey, *supra* note 1.

¹³ Alfred Moore, *Anonymity, Pseudonymity, and Deliberation: Why Not Everything Should Be Connected*, 26 J. Pol. Phil. 169 (2018).

¹⁴ *Why India Is Concerned About WhatsApp Usernames and What It Could Mean for Other Countries*, *supra* note 2.

behind usernames creates possible risk of identity theft, impersonation, cyber fraud, and making traceability difficult by adding one additional step to detection.

Some experts and digital rights groups argue that the government's notice to Meta has no clear basis in law under existing technological rules. The government has reportedly cited the definition of an intermediary under Section 2(1)(w) of the IT act, 2000, together with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, under which WhatsApp qualifies as a Significant Social Media Intermediary owing to its large user base. Therefore, it makes the platform subject to the due diligence set out under the rules of the act.¹⁵ This raises an important legal question – How should the government respond to a new technological feature if it simultaneously enhances user privacy and creates new enforcement challenges or possible future risks? Therefore, future regulations must seek to protect informational privacy without putting unnecessary restrictions on positive technological innovations.

CONCLUSION

The introduction of usernames is an important step towards giving users more control over their personal data and digital identity. This also indicates that privacy is becoming a part of the platform design itself and enhancing it has become a central idea not just in case of companies but also for the government. These developments suggest that Indian privacy law will need to balance user autonomy, privacy, as well as technological innovations while keeping security and public safety in mind. However, not only the legal framework, the companies themselves would need to balance innovation with proper accountability as projected in the DPDP Act, 2023.

¹⁵ Information Technology Act, No. 21 of 2000, § 2(1)(w) (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 2(1)(v), 4.