PATENTS, PIXELS, AND PROFILES: REASSESSING INTELLECTUAL PROPERTY AND PRIVACY IN QR-BASED IDENTIFICATION

Ms. Khushi Ruchandani*

Abstract

In today's fast paced and digitalized work, interactions are more virtual than they were previously. Social media platforms have simplified this process even further by introducing scannable identity markers like QR codes, Snapcodes, and NameTags, found across social media platforms. These markers enable users to instantly access profiles of other users and initiate chats as well and it eliminates the need of manually saving contact details. While these features have been designed for efficiency, they involve layered challenges. On one hand, they raise concerns related to intellectual property as to how should we treat the interface or underlying code and whether they are protected by intellectual property laws? On the other hand, the privacy dimension of this is equally relevant as these codes encode within themselves identifiable data of a user. In this paper, the researcher explores these intersecting legal dimensions. by analysing the status of QRs in IP laws and the privacy implications under the Digital Personal Data Protection Act, 2023. The paper showcases how different social media interfaces operate within frameworks. The analysis suggests that these identity tools functions more than digital shortcuts. They exist at the intersection of user data and proprietary framework which gives rise to concerns about ownership, control and consent. As platforms continue to experiment with these features, it becomes essential to ensure that innovation does not outpace the twin legal pillars of intellectual property and data protection.

Keywords: *Data Protection, Digital Identity, Intellectual Property, Privacy Law, QR Codes.*

INTRODUCTION

In the 21st century, personal identity is anything but personal. Every human being has now been assigned QR codes that serve as our labels. People often refer themselves by their usernames

* Final-year student BA.LL.B(Hons. in Adjudication and Justicing), Maharashtra National Law University, Nagpur.

and not names. Regular things like making payments or initiating conversations are not done saving contacts but through scanning codes. These include not only the familiar QR (Quick codes, but also platform-specific innovations like Snapchat's Snapcode, Instagram's Nametag etc. These innovations while time-efficient are not IP-efficient. They raise serious questions like: Can the design of a Snapcode be copied? Is the structure of Nametag of Instagram protectable under Design or Copyright law? Beyond these IP concerns lies another domain of issue i.e. privacy law. Scannable codes carry all the details of the user and their use, storage, and potential distribution trigger obligation under privacy laws. A code may be protected as creative output under copyright, yet the information it carries may be governed by entirely different rules under privacy law. This is what makes this intersection particulary interesting and these questions are analysed and answered within the scope of this paper through a dual lens. First, it analyzes the origin and current IP status of visual code technologies, particularly QR codes, Snapcodes, and Nametags. Second, it examines the privacy implications of user-generated code sharing, with particular attention to India's IP laws. The paper concludes that user-centric design must harmonize with emerging obligations in digital rights management and data protection.

1. QR CODES AND SCANNABLE IDENTIFIERS: ORIGIN AND LEGAL STATUS

The QR code was developed in 1994 by Japanese firm Denso Wave, originally to streamline inventory tracking in the automotive industry.[1] Its two-dimensional square grid could hold significantly more information than traditional barcodes and could be scanned from any angle, making it revolutionary for logistics and packaging. What set QR codes apart from the start was Denso's deliberate decision not to monetize the patent aggressively. While the company filed patents (e.g. JP2938338), it publicly declared that it would not enforce them, provided users complied with basic brand guidelines. This decision enabled widespread adoption and standardization, culminating in ISO/IEC 18004, the global technical standard for QR codes.

Today, QR codes are freely used across industries, from payments and product tracking to vaccination records and social media. However, Denso retained trademark rights over the term "QR Code"**,** particularly in Japan and other jurisdictions. As per Japanese Patent Office documentation, users must include a disclaimer such as "*QR Code is a registered trademark of*

[1] Denso Wave, "About QR Code," available at: https://www.denso-wave.com/en/adqr/about/ (last visited on June 18, 2025).

DENSO WAVE INC." when referring to the code commercially. Thus, while the matrix technology is non-proprietary, the branding is protected. In contrast, Snapchat created Snapcodes, which although inspired by QR codes, use a proprietary dotted matrix system. Snap Inc. holds multiple US patents on Snapcode technologies and visual formats. In addition, Snap has registered trademarks over the Snapcode name and design, giving it robust IP control over both functionality and form.[2] These protections prevent third parties from replicating Snapcode's exact visual interface or back-end encoding method.

Instagram's Nametag lies somewhere between WhatsApp's open QR system and Snap's proprietary model. While Instagram does not use a traditional QR grid, it provides a stylized scannable tag that launches the user's profile. Its layout, often featuring pastel colour palettes, emojis, and font variations, is designed for aesthetic distinctiveness, not information density. Legally, it likely enjoys copyright protection for the graphical layout and design protection under India's Designs Act.[3] However, Instagram has not asserted any exclusive encoding method, and Nametags are not known to be protected.[4] Telegram's QR contact link, on the other hand, adopts a pure ISO-standard QR matrix. Each code simply encodes a URL to the user's t.me link. It is open, simple, and adheres strictly to interoperable standards. Telegram adds little proprietary design, branding, or encoded data beyond the link itself. This simplicity means that Telegram's system carries minimal IP risk but also minimal protection. Its strength lies in privacy, not proprietary tech. These origin stories highlight a spectrum of legal approaches: from open standard (Telegram, WhatsApp) to stylized copyright/design protection (Instagram), to full-stack IP control (Snapchat). For legal analysts, this raises a key question: does the format and layout of a code make it protectable under IP laws, and if yes, to what extent?

2. LEGAL FRAMEWORK IN INDIA

India's legal system provides a rich yet evolving framework for addressing the complexities of QR-based identity codes. This framework draws on four primary legal domains: copyright,

[2] Snap Inc., "Snapcode with Augmented Reality," US Patent No. 9,369,544 (May 3, 2016).
[3] The Designs Act, 2000 (Act 16 of 2000), published in the Gazette of India, Extraordinary, Part II, s. 1 (May 25, 2000).
[4] Meta Platforms Inc., "About Copyright," Instagram Help Center, available at: https://help.instagram.com/126382350847838 (last visited on June 18, 2025).

design, patents, and data protection. Each regime interacts with scannable identity interfaces in nuanced ways, depending on whether the subject is a visual layout, a code format, a functional process, or personal data embedded in the code.

2.1 Copyright and Design Protection

Under the Copyright Act, 1957, software code is protectable as a literary work. Graphical user interfaces (GUIs) and screen designs may also qualify as artistic works under Section 2(c). In the case of QR-based identification, elements such as the user interface used to generate, display, or scan the code, including icons, frames, animations, or stylised elements, can be protected under copyright if they exhibit originality and are fixed in a tangible medium.[5] For instance, WhatsApp's QR generation screen, with its familiar green branding and layout, or Instagram's pastel-coloured Nametag interface, likely qualify as copyrightable expressions. However, copyright does not protect ideas or functional elements. Therefore, the core QR matrix itself (black-and-white squares encoding data) is unprotectable under Indian law.

Further protection may arise under the Designs Act, 2000. This act defines "design" in Section 2(d) as the features of shape, configuration, pattern, or ornamentation applied to any article by any industrial process.[6] Notably, in 2008, India adopted Locarno Classification Class 14-04, which explicitly includes "screen displays and GUIs." This paved the way for the registration of digital screen layouts, including those used in QR code display interfaces. The Indian Patent Office's application of the Designs Act to GUIs has been inconsistent. In 2015, Amazon's design registration for a GUI was refused because GUIs lack physical embodiment when a device is off, making them not considered "articles." However, successful GUI design registrations by Microsoft suggest that a QR-display GUI could be registrable with a strong application demonstrating industrial application and visibility during use. While copyright protection offers immediate, automatic protection upon creation, design registration provides additional enforceability, albeit subject to examination and procedural uncertainty.

2.2 Patentability of QRs

The Patents Act, 1970 permits registration of novel, non-obvious inventions with industrial applicability. Under §2(1)(j), an "invention" must demonstrate novelty, inventive step, and industrial application. At the same time, §3(k) excludes "a mathematical or business method or

[5] The Copyright Act, 1957 (Act 14 of 1957), s. 2(c).
[6] The Designs Act, 2000 (Act 16 of 2000), s. 2(d).

a computer programme per se or algorithms" from patentability unless the claimed subject-matter produces a demonstrable technical effect or is tied to hardware functionality.[7] While the original QR code inventions were patented by Denso Wave in Japan, those patents have expired or been opened to public use. Today, platforms using ISO-standard QR codes, such as WhatsApp or Telegram, face no patent liability. However, platforms may still patent new methods of encoding, personalisation, or verification within such codes. For instance, Snapchat's Snapcode patent portfolio includes proprietary encoding mechanisms, use of augmented reality (AR), and visual processing. Indian jurisprudence illustrates this balance: in *Ferid Allani v. Union of India*,[8] the court held that computer-related inventions producing a technical contribution could be patentable notwithstanding §3(k). Conversely, in *Yahoo Inc. v. Controller of Patents,*[9] the tribunal rejected claims relating to online advertising as falling within the exclusion.

In India, such methods may be patentable if they result in a technical advancement, such as secure identity verification through facial overlays or unique animations triggered by a code scan. In practice, WhatsApp and Instagram do not appear to have sought Indian patents for their code systems, possibly because they rely on known methods and visual design rather than technical novelty. However, if either introduces QR encryption, device authentication via QR, or dynamic data flows, they could claim patent rights. The enforceability of such rights flows from §48 of the Act, which grants exclusive rights over patented products and processes. In Telefonaktiebolaget LM Ericsson v. Intex Technologies,[10] the court emphasised the strength of patentees' rights in standard-essential technologies, and in Enercon (India) Ltd. v. Aloys Wobben, the Supreme Court clarified the scope of protection available under §48. These decisions underline that QR-related patents, once granted, would provide enforceable exclusivity against unauthorised commercial use.

2.3 Trademark and Trade Dress

Under the Trade Marks Act, 1999, logos and names used in relation to goods or services can be protected as trademarks.[11] This becomes relevant when a code includes a branded overlay,

[7] The Patents Act, 1970 (Act 39 of 1970), s. 3(k).
[8] Ferid Allani v. Union of India , 2019 SCC OnLine Del 11836.
[9] Yahoo! Inc. v. Controller of Patents, 2012 (49) PTC 502 (IPAB).
[10] Telefonaktiebolaget LM Ericsson v. Intex Technologies, 2023:DHC:2243-DB.
[11] The Trade Marks Act, 1999 (Act 47 of 1999), s. 2(zb).

such as Snapchat's ghost logo within its Snapcode or WhatsApp's logo surrounding its QR interface. Instagram's Nametag design may also qualify for trade dress protection, which safeguards non-functional visual aspects that indicate source or brand identity. For instance, if the layout, colours, and aesthetic of a Nametag become associated with Instagram's services, they may acquire distinctiveness over time.

2.4 Privacy laws.

One of the most significant legal developments influencing the use of scannable tools in India is the Digital Personal Data Protection Act, 2023 **("DPDP Act, 2023").**[12] Section 2(i) of the DPDP Act, 2023 defines personal data as "*any data about an individual who is identifiable by or in relation to such data."* In this context, all social media platforms are enaging in data processing under the Act by embedding users details into those black and white boxes. As per Section 4 of the DPDP Act, 2023 any such processing should have a lawful basis attached to it and another layer is added by Section 6 by stating that users should be clearly informed about the purpose of data collection, the type of data involved and the concerned fiduciary. The DPDP Rules further operationalise these provisions by prescribing the format and language of notices, requiring them to be clear, concise, and accessible to the average user.[13] They also emphasise that consent must be granular, allowing users to agree to one category of processing while declining others.

Although an individual may be voluntarily requesting you to scan a code on their application, it does not imply that the platform is exempt from legal regulations governing automated behaviour. Like, saving a contact or recommending engagements with other users through a scan is considered valid. Furthermore, if the scanned data is subsequently utilised at a later stage as an input to analytics, behavioural profiling, or, crucially, even cross-service integration (e.g., from Meta's family of services including WhatsApp and Instagram), the DPDP Act would necessitate an specific and informed consent.[14] Under the DPDP Rules, cross-platform or secondary processing requires a fresh and separate consent, and significant data fiduciaries are obliged to conduct Data Protection Impact Assessments before implementing such features.

Data fiduciaries, which encompass major platforms such as Meta, Snapchat, and Telegram (excluding WhatsApp), are expected to adhere to fundamental principles of purpose limitation, data minimisation, and storage limitation. The DPDP Rules reinforce these duties by requiring

[12] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(i), 4, 6.
[13] The Digital Personal Data Protection Rules, 2023, r. 4.
[14] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 6(3).

Significant Data Fiduciaries to appoint a Data Protection Officer, establish grievance redressal timelines, and subject themselves to regular audits. Rule-based obligations therefore transform the general principles of the Act into enforceable compliance mechanisms. If platforms fail to provide tools such as QR resets, timed codes, or user-side alerts upon reading, this could potentially result in their violation of the DPDP Act. Hence, this nuances are there which needs to be complied with.

3. PLATFORM ANALYSIS

a. Whatsapp

The QR based identity feature in WhatsApp provides ease of operation with. intricate legal implications. The feature called "WhatsApp Profile QR Code" generates a static QR code for each user. This code encodes a wa. me URL that contains the phone number of the user. Once scanned by another WhatsApp user, it automatically nabs the other's personal details. and opens a chat window while saving the user in contact list. This takes away the need to enter it manually improving user convenience. However, it raises significant considerations under intellectual property law. The QR matrix adheres to the ISO/IEC 18004 standard and is part of the public domain, meaning it is not subject to proprietary rights. Conversely, WhatsApp's presentation of the code, including its user interface design, green-tinted colour scheme, layout, and branding elements, is proprietary. These elements are likely protected under copyright law as original artistic and software expressions. Additionally, if WhatsApp incorporates its logo or watermark within or around the QR code, those components are protected under trademark law. The overall visual presentation of the QR interface may also be eligible for design registration under India's Designs Act, 2000, particularly under Locarno Class 14-04 (screen displays and GUIs), although there is no public record of such filings by WhatsApp in India.[15]

Under privacy law, scanning the code exposes a user's phone number, which qualifies as personal data under the DPDP Act, 2023. Since the sharing is user-initiated, consent is implied, but only to the intended recipient. If a third party screenshots and redistributes the QR, it results in unauthorised processing. WhatsApp does provide a "Reset QR Code" feature, enabling users to invalidate old codes, aligning with data minimization and user control principles under DPDP. However, legal ambiguity remains around what constitutes "implied consent" and

[15] Controller General of Patents, Designs and Trademarks, "Manual of Designs Practice and Procedure," available at: https://ipindia.gov.in (last visited on June 18, 2025).

whether mere display of a QR satisfies the obligation under Section 6 to inform users of processing purpose and scope.

b. Instagram

Instagram introduced its Nametag feature in 2018 as a visually stylised scannable identifier. Accessible under the profile menu, Nametags allow users to scan each other and open a profile. Unlike WhatsApp, no phone number is embedded in the tag, which contains a stylised graphical pattern overlaid with the user's Instagram handle. From an IP perspective, the visual layout of Nametags is distinctive and likely protected under copyright and design law. Although not known to be patented, the visual coding method and scan interface qualify as creative expression. Instagram's prominent branding also suggests that the interface could be protected under trade dress. From a privacy standpoint, since only the username is revealed, the privacy risks associated with scanning a Nametag are lower. Instagram accounts are often public, and scanning a Nametag merely replicates a public search. However, if the tag were posted without consent or used for automated scanning, it could constitute unauthorised profiling, especially if coupled with metadata extraction. Importantly, Instagram allows users to reset their Nametag or switch to different styles, offering users a degree of revocability and customization, which aligns with DPDP expectations.

c. Snapchat

Snapchat's Snapcode is perhaps the most legally fortified of all platforms. Introduced in 2015, each Snapcode comprises a yellow square, a central ghost logo, and a dotted matrix surrounding the avatar. Scanning a Snapcode leads to a connection request, friend suggestion, or content unlock, depending on the context. From an IP law perspective, Snap Inc. holds multiple US patents (e.g., US Patent No. 9,369,544) on the structure and underlying technology of Snapcode.[16] The Snapcode name and visual layout are also registered as trademarks, and any copying of Snap's distinctive yellow-black layout would constitute infringement. The design, animation, and code-use structure of Snapcode also qualify for protection under copyright and possibly design law. From a privacy law perspective, Snapcodes reveal only usernames, not phone numbers or emails. Scanning a Snapcode triggers a request, not an automatic connection, ensuring user control. Snapchat, targeting a young demographic, incorporates privacy by design, including ephemeral content and opt-in connections. Snap's layered IP protection strategy makes Snapcodes not only functional but also monetisable

[16] Snap Inc., "Snapcode with Augmented Reality," US Patent No. 9,369,544 (May 3, 2016).

branding assets. The platform uses them to link to promotional content, AR lenses, and third-party integrations, further reinforcing their proprietary status.

d. Telegram

Telegram's QR implementation is simple. Each user has a QR code linking to their t.me/username. Users can scan this QR code in Telegram to open their profile. Telegram uses standard QR codes, offering no unique matrix or design innovation. The layout is minimal, with no proprietary symbols or design, so there's little scope for copyright. There's no public evidence of design or patent filings by Telegram in India or globally. By default, Telegram uses usernames instead of phone numbers for QR codes. Users can hide phone numbers, block uninvited users, or change usernames, giving them substantial control. QR code-generated connections are user-controlled and require approval before interaction, satisfying DPDP consent principles. Telegram's approach prioritises privacy and simplicity over proprietary innovation. The next section compares these approaches to assess how effectively they comply with intellectual property and data protection law.

4. COMPARATIVE LEGAL IMPLICATIONS

When taken together, WhatsApp, Instagram, Snapchat, and Telegram show four different methods of scannable identity systems and each of them exhibits a different level of balance between assertion of intellectual property rights and user control over privacy. Snapchat takes the most upfront intellectual property position as its Snapcode system is defended using patents, trademarks, and design registrations, giving proprietary control over both visual design and underlying encoding method to the company. Instagram, however, uses a design-led model and its Nametag tool, although not patented, employs stylised, copyrightable interfaces that almost certainly entitle to design protection and trade dress. This model provides branding benefit with minimal risk of infringement. Whereas, WhatsApp uses a generic QR format and uses minimal proprietary design and while its user interface is copyrightable, its underlying code design is in the public domain.

Moving to the privacy aspect of these apps, the sites' processing of users' data discloses contradictory privacy policies. To begin with, WhatsApp's QR code stores users' phone numbers explicitly, with the highest risk of exposure. This is particularly problematic in terms of consent, minimisation, and legal processing under the DPDP Act, 2023. On the other hand, Instagram and Snapchat employ usernames or handles, which are non-sensitive identifiers that

can easily be reset or anonymised and, at last, Telegram offers the most control to users, enabling them to conceal their phone numbers, limit scanning, or modify usernames entirely. As opposed to WhatsApp's, Telegram's approach is more organically grounded in the DPDP values of data minimisation and user control and such deviations are indicative of larger platform ideologies. Significantly, Indian law accommodates all of these models but requires a uniform level of transparency, consent, and governance of data. A proprietary Snapcode employed in India must nonetheless conform to the DPDP Act's requirements for processing, and even an open system such as Telegram must ensure that user data gathered by QR scanning is processed legally. Finally, this reflects the imperative for platforms to balance IP strategy and privacy requirements together, particularly as India's legal framework becomes increasingly rights- and enforcement-oriented in this new age.

5. RISKS AND REGULATORY RESPONSES

As QR code have become a part of our daily life due to the ease they provide us however we should also be aware of the risks they bring with them. The Indian legal framework, particularly after the enactment of the Digital Personal Data Protection Act, 2023 (DPDP), demands that platforms address these risks through privacy-focused design and active compliance measures. A major concern is the unintended disclosure of the personal data. For example, although a person might have volunatary shared their code to someone on whatsapp, however, it can easily be stored or shared without the user's consent. While whatsapp offers reset QR code option, this only protects any future misoccurences and cannot undo and get back the personal data of the user.

The next risk is the issue of scraping and profiling. Bots can collect these codes, especially in Telegram and connect it to user profiles and build identity graphs without any form of consent. While scraping data might not always be a copyright violation, it often goes against the terms of service and could even be considered unauthorised data processing under the DPDP Act, 2023. The act makes it clear that data collection should have a specific, legal purpose, and bulk harvesting of user codes doesn't quite fit that standard. Another issue is added to this long list by spoofing and impersonation. Fake QR codes can be created that look mostly similar to the legitimate ones whicb tricks users to malicious links and scams. Although Indian law does not currently include a provision specifically addressing QR code forgery, the Information Technology Act, 2000, along with intermediary liability guidelines, can be invoked to take

necessary actions like takedowns and penalties.[17] In addition, Section 65A of the Copyright Act provides recourse when digital security features, such as QR encryption, are bypassed or altered.[18]

Another significant concern which was also highlighted by Competition Commission of India and has flagged by them as being anti-competitive is cross platform data sharing which is very easy through these QR codes.[19] We always see that our activities are tracked across different apps because these codes allow and create unified user profiles. Under the DPDP, any such data sharing requires clear, informed, and separate consent. To mitigate these risks, platforms must implement safeguards such as QR expiration timers, scan alerts, access logs, and user-facing notices among the others to begin with. The key shift required is a move from treating scannable codes as mere features to recognising them as potential vectors of data exposure. In short, offering convenience is no longer enough and compliance and privacy by default must guide every step of how identity systems are designed and deployed in this digital age where all of us have wore a virtual mask, namely, QR or identity codes.

6. ANALYSIS

A well-known aphorism states, "*The more we define ourselves through technology, the more it defines us*." This paper elucidates that scannable identifiers, such as QR Codes, Snapcodes, and Nametags, intersect intellectual property and privacy law. Platforms exercise exclusive rights over the visual design and encoding of these identifiers through copyright, design, trademark, and even patents under sections 2(1)(j), 3(k), 10(4), and 48 of the Patents Act, 1970. Simultaneously, the Digital Personal Data Protection Act, 2023 ("DPDP Act") and its Rules impose obligations of notice, consent, minimisation, and grievance redressal whenever these identifiers process personal data. Indian courts have already clarified, in *Ferid Allani v. Union of India*[20] and *Yahoo! Inc. v. Controller of Patents*,[21] that computer-related inventions may be patentable only if they demonstrate a demonstrable technical effect, thereby underscoring the narrow path such technologies must navigate. The analysis further reveals a spectrum of compliance: WhatsApp exposes sensitive phone numbers, Instagram and Snapchat restrict identifiers to usernames, while Telegram prioritises user control. Each model engages privacy

[17] The Information Technology Act, 2000, s. 79; Intermediary Guidelines, 2021.
[18] The Copyright Act, 1957 (Act 14 of 1957), s. 65A.
[19] Competition Commission of India, "Suo Motu Case No. 01 of 2021.
[20] Ferid Allani v UOI, 2014 SCC OnLine Del 1825.
[21] Yahoo! Inc. v. Controller of Patents, 2012 (49) PTC 502 (IPAB).

differently, but all fall within the DPDP Act's consent regime and its Rules on significant data fiduciaries, audits, and grievance mechanisms. Thus, the legal challenge is to ensure that what platforms claim to own as proprietary "code" does not override the user's fundamental right to informational privacy under Article 21 of the Constitution.

7. CONCLUSION AND SUGGESTIONS

A more integrated framework is required moving forward. The Patent Office, while examining applications relating to scannable identifiers, should embed privacy considerations within its assessment of computer-related inventions. For instance, applicants could be required to disclose privacy-preserving features, such as encryption, expiry timers, or reset mechanisms, before obtaining patent rights. This would align IP protections with the principle of "privacy by design" and prevent purely proprietary innovations from being privileged over user rights. Similarly, the DPDP Rules should be amended to expressly mandate the inclusion of expiry, scan alerts, and grievance channels in identity codes, thereby operationalising consent and purpose limitation obligations in practice.

Additionally, Indian law must confront emergent risks such as forgery and cross-platform profiling. The *Information Technology Act, 2000* could be amended to recognise QR code forgery as a specific cyber offence, akin to digital signature falsification. Cross-service integration, particularly in conglomerate platforms like Meta, should be subjected to stricter consent requirements under the DPDP Rules, demanding separate and informed permissions for each instance of data linkage. This would prevent platforms from expanding proprietary rights into unchecked surveillance, while also safeguarding competition and user autonomy.

Finally, a cross-regulatory mechanism is necessary. IP India and the Data Protection Board should establish a formal review channel for technologies that implicate both intellectual property and personal data. Such coordination could produce joint guidelines clarifying that IP protection of scannable identifiers does not extend to the personal information encoded within them. At the same time, a limited safe harbour could be introduced in IP law, permitting research, interoperability, and privacy-enhancing uses of such identifiers without liability. In this way, Indian law can reconcile "code as property" with "code as person," setting a global precedent for regulating digital identity systems in a manner that honours both innovation and constitutional privacy rights.

To conclude it is submitted that scannable identifiers are no longer mere digital conveniences but socio-legal constructs. Recognising them simultaneously as protectable innovations and as carriers of personal identity requires an integrated regulatory approach. By aligning intellectual property protections with privacy-by-design obligations, India can set a global benchmark in governing the future of digital identity systems.