LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

JULY & AUGUST
2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

BROADCASTING BILL 2023 AND ITS IMPACT ON DIGITAL MEDIA CREATORS

NEWS

On August 12, 2024, the Ministry of Information and Broadcasting withdrew the new draft Broadcasting Services Regulation Bill 2023 which triggered a controversy and criticism over fears that the government was trying to exert greater control over online content. The recent draft Bill has raised several questions on the freedom of speech and expression and the threat to media independence.

THE WAY FORWARD

Although still being in its early stages, the Bill is an essential step towards regulating online media content to keep a reasonable check on the news, however, the Bill could have taken a more balanced and nuanced approach similar to that of the EU, upholding free speech and expression and freedom of online content media creators, in order to represent the spirit of free speech and expression without breaching any of it. Moreover, the Bill's purview could be reduced to mainly target larger broadcasters, with specific and appropriate regulatory standards. These changes will better support a robust media and content creation industry in India.

LEGAL TALK

Free media is a key pillar of every democracy and it is essential for a healthy market economy. The Broadcast Bill, 2023 seeks to replace the Cable Television Networks Regulation Act, 1995, by bringing substantial changes to the regulation of broadcasting and online content in India. The Bill has defined digital news broadcasters in s. 2 (i) as, "*a person who provides programming services and has been provided a registration under Section 11 for uplinking or downlinking of programmes, and in relation to Radio, OTT and Terrestrial broadcasting network, means the operator of such service;*". This has been defined in a non-exhaustive manner thus expanding its scope to include social media accounts and online video creators to cover anyone monetising news and current affairs online which includes digital content from newspapers and those sharing news on platforms like YouTube, Instagram or even X (formerly Twitter). The compulsory registration with the government before creating content raises serious concerns as it can result in censorship and limit free speech and it also puts privacy and safety of the creators at risk especially that of teenagers and female creators. Additionally, it aims to implement the IT Rules, 2021, which have already drawn criticism from Courts for putting unreasonable limitations on free speech by using ambiguous and broad language. Recently, frameworks such as the European Media Freedom Act (EMFA) of the EU have been implemented to protect media freedom and pluralism in the EU, in addition to enhancing free movement of services. While the Bill focuses on control, with broader, strict criteria and a lack of transparency in its working, the EU's Act promotes freedom of expression, self-regulation, and collaboration. The Bill also seeks to control current affair news programs by imposing severe penalties on noncompliance, up to 2.5 crore rupees for repetitive breach. Additionally, Its broad and ambiguous wordings might potentially include foreign content creators, raising questions regarding its enforceability.

TELECOM OPERATORS URGE TELECOM REGULATORY AUTHORITY OF INDIA TO DESIGN A LICENSING REGIME FOR OTT COMMUNICATION APPS

NEWS

Numerous telecom operators, including Reliance Jio, Airtel, and Vodafone, have called for Telecom Regulatory Authority of India ("**TRAI**") to bring call and over-the-top ("**OTT**") messaging services like Whatsapp, Facebook Messenger, and Telegram under the new Telecommunication Act's licensing framework.

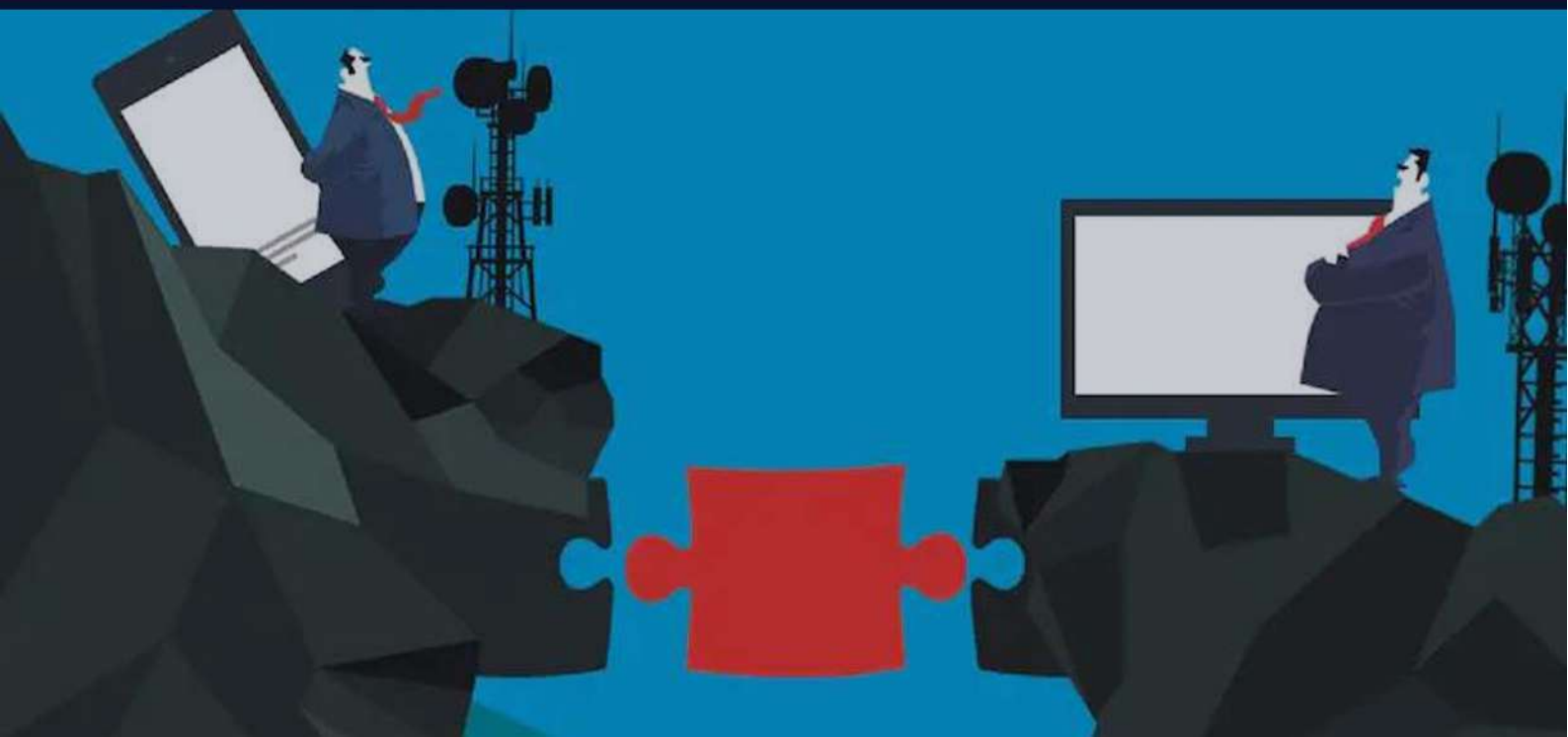
LEGAL TALK

The telecom sector in India is heavily regulated requiring operators to obtain licences, pay spectrum fees and comply with various regulations. On the other hand, OTT communication services operate with minimal regulation, relying on the existing telecom infrastructure. This allows them to offer competitive services, without the associated cost and compliance. Telecom operators are advocating for regulatory parity and contend that the current regulatory landscape leads to unfair competition and revenue loss. A licensing regime could force OTT platforms to conform to strict telecom regulation, including service standards, data localization and possibly even lawful interception and monitoring requirements. Such a step could impede smaller players, imposing heavy compliance costs and enabling market consolidation. It also raises numerous privacy concerns and could lead to weakened encryption standards and increased surveillance. Further, increasing compliance costs could also be passed down to customers, leading to higher service costs, and lower revenues for both OTT platforms and telecom companies. Opposing factions are challenging the extent to which OTT platforms are covered under the new Telecommunication Act. Telecom companies are contending that OTT platforms are covered under the new act as an 'access service' and demand 'same service same rules' for OTT platforms. On the other hand, OTTs have stressed that they only operate at the application layer, as opposed to telecoms operating at the network layer. The debate hinges on how OTT platforms and telecom operators are defined under various legislative frameworks. In India, OTT platforms are primarily governed under the Information Technology Act, 2000, which deals with electronic communication and data protection, whereas telecom operators fall under the ambit of the Telegraph Act, 1885, and the new Telecommunication Act.

The latter involves a stricter licensing regime and compliance requirements like spectrum fees, service standards, and interception capabilities. This regulatory disparity stems from their differing roles: telecom operators provide the physical network layer, while OTTs operate at the application layer, delivering services that run on these networks. Different jurisdictions have approached this issue in varied ways. For instance, the EU's Electronic Communications Code aims to bring certain OTT services under a common regulatory framework with traditional telecom operators by defining 'number-independent interpersonal communications services.' This brings specific OTT services under a modified form of regulation that focuses on security and interoperability but not necessarily on full licensing parity. The United States, on the other hand, has largely kept OTT platforms outside the purview of telecom regulations, emphasising innovation and consumer choice. Given these definitions and global approaches, a critical question arises: Can OTT platforms and telecom services be regulated under a single umbrella in India, or does their distinct functional nature require different regulatory treatment? While telecom operators argue for 'same service, same rules,' OTT platforms contend that their role in the digital ecosystem complements rather than competes with traditional telecom services, warranting differentiated treatment.

THE WAY FORWARD

As TRAI designs novel regulatory frameworks, it must strike a balance between the interests of telecom operators, OTT platforms, and user requirements. A potential outcome also discussed in the TRAI's consultation paper, could involve a tiered licensing system, where larger service providers are subject to more strict regulations, with smaller players enjoying less stringent oversight. This would ensure a more level playing field, while preventing overregulation that could stifle innovation and deter newer players. As digital ecosystems converge, should regulations be designed to treat all data carriers–whether telecoms or OTT platforms–equally in terms of obligations of responsibilities? Or, should innovation and user protection remain the central principle, even at the cost of regulatory parity? Officials indicate that TRAI will be providing clarity on the matter later this month.



KARNATAKA'S WELFARE FUND FOR CINE AND CULTURAL ACTIVISTS

NEWS

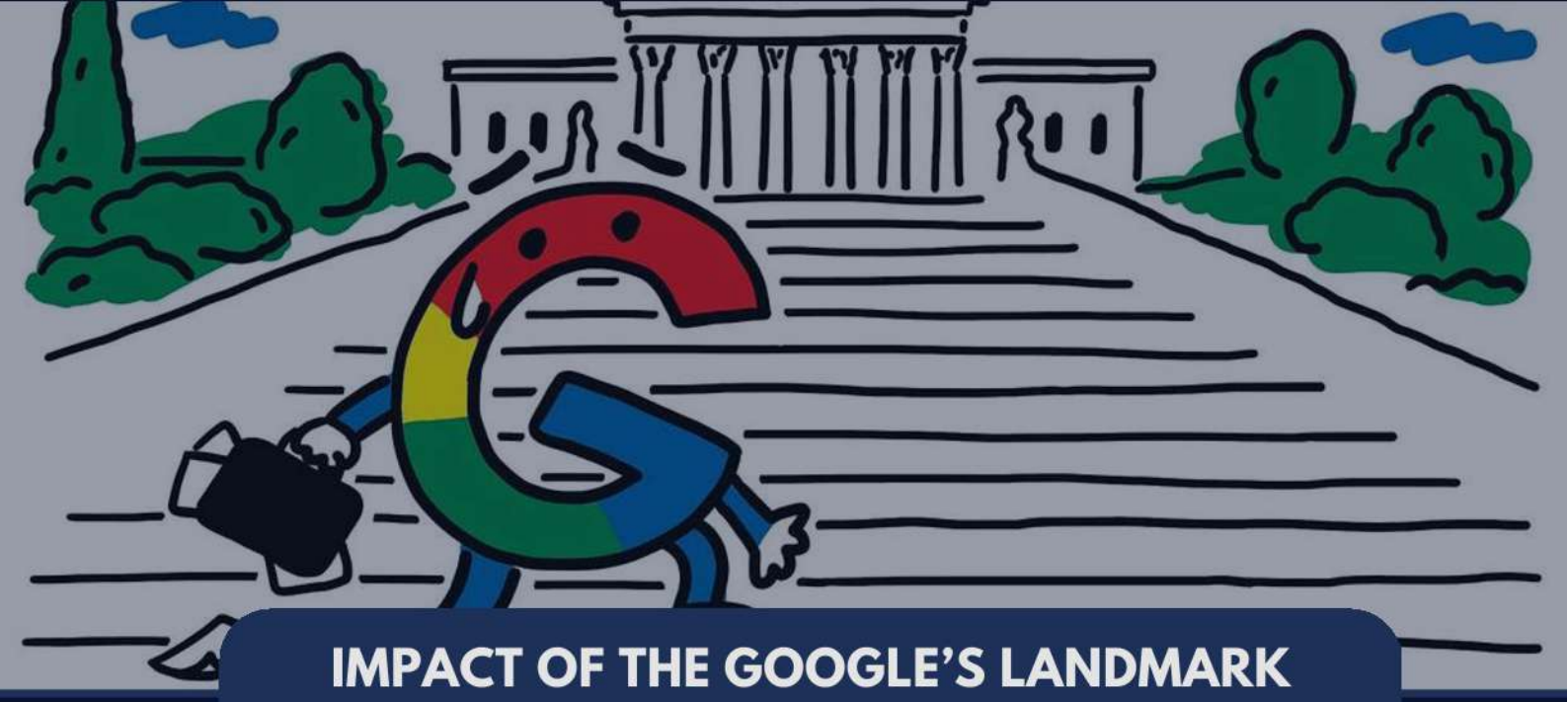
The Karnataka Government has tabled the Karnataka Cine and Cultural Activists (Welfare) Bill, 2024 ("the Bill"), seeking to provide social security to Cine and Cultural activists by establishing a welfare fund. This welfare fund shall consist of the cess applied, contributions received from registered activists, and aid and funds received by the Government.

LEGAL TALK

The Bill aims to provide welfare to Cine and Cultural activists which is defined under Section 2 (e) as any person who is employed concerning the field of cinema to work as an artist (including actor, musician, or dancer) or to do any work, skilled, unskilled, manual supervisory, technical, artistic or otherwise or any person who is being engaged in such other activities as declared by the government. It proposes a 1-2% welfare cess on cinema tickets, subscription fees, and all revenue generated by related establishments in Karnataka, which include cinema theatres, multiplexes, OTT platforms, and television channels as defined Section 2(o) of the Bill. However, the Bill seems vague about the revenue-generating activities that shall be subject to this cess. While subscriptions are a primary revenue source for streaming platforms, other income streams like promotions, fan events, special screenings, content licensing, and telecom partnerships are also significant. The Bill also lacks clarity on how it will identify Karnataka-based subscribers for imposing cess on subscriptions of OTT platforms, potentially leading to new regulatory burdens and compliance costs.

THE WAY FORWARD

While the cess aims to support welfare in the cultural sector, the government appears more focused on quickly boosting revenue. This could stifle a thriving entertainment market, potentially deterring investment and innovation in the state. A more balanced approach would be to fund social welfare without burdening consumers and businesses. Additionally, the cess could make leisure activities more expensive, reducing the access to entertainment for people from lower-income backgrounds. Moreover, the Bill lacks clarity on how the cess will be imposed on OTT platform subscriptions and whether it will necessitate revising rates specifically for residents of the state.



IMPACT OF THE GOOGLE'S LANDMARK ANTITRUST RULING ON TECH COMPETITION

NEWS

The technological landscape has long been dominated by a handful of giants, with Google frequently at the centre of discussions surrounding monopolistic practices. In recent years, Google's stranglehold on the search engine market and its broader digital advertising empire has attracted scrutiny from regulators and competitors alike. The U.S. District Court has held that Google has engaged in anti-competitive practices to maintain and extend its market dominance. Tactics such as prioritising its own services in search results, entering exclusive agreements with mobile manufacturers to pre-install Google apps, and acquiring potential competitors before they can become significant threats have all contributed to the growing call for regulatory intervention. The latest antitrust ruling against Google marks a pivotal moment, not only in the tech giant's history but also in the broader narrative of how governments seek to regulate the power of Big Tech.

INFLUENCE ON TECH COMPETITION

Breaking up Google could significantly alter the competitive landscape in the tech industry. On the one hand, it could lead to increased competition as new players enter markets previously dominated by Google, potentially benefiting consumers through lower prices and better services. The fragmentation of Google's vast ecosystem might also inspire innovation, as smaller companies could focus on niche areas without the overarching influence of a tech giant. This increase in competition could foster a more diverse and dynamic market environment. However, there are also potential downsides. The disruption of Google's integrated ecosystem could lead to a fragmented user experience, where services that once worked seamlessly together might no longer do so. Moreover, the economic impact of such a breakup could be significant, with potential job losses and reduced investments across the industry. Furthermore, setting a precedent for breaking up large tech companies might lead to over-regulation, potentially stifling innovation as companies become more cautious in their expansion efforts.

OTHER SIMILAR LAWSUITS

Google is not alone in facing antitrust scrutiny, as other tech giants like Amazon, Apple, and Meta have also encountered significant legal challenges. Amazon has been accused of leveraging its platform to prioritise its own products and using third-party seller data to create competing products, raising concerns about reduced consumer choice and stifled competition. Meanwhile, Apple's App Store policies, particularly its 30% commission on in-app purchases, have been criticised for being anti-competitive, with developers arguing that Apple exercises too much control over the app economy. Meta's situation involves allegations of acquiring potential competitors, such as Instagram and WhatsApp, to maintain its dominance in social media and messaging markets. This strategy has drawn criticism for preventing competition and consolidating power within a few key platforms. Additionally, ongoing concerns over data privacy and misinformation have intensified the scrutiny on Meta, further highlighting the challenges these companies face as they navigate the increasingly complex regulatory landscape. Each of these lawsuits reflects a broader movement to rein in Big Tech's power and ensure fair competition in the digital marketplace.

THE WAY FORWARD

While breaking up the tech giant Google might seem like a straightforward solution to restoring competition, it also poses significant risks and challenges. The potential for unintended consequences, such as market disruptions and stifled innovation, cannot be ignored. Moving forward, regulators must strike a balance between curbing monopolistic practices and fostering an environment where innovation can thrive. This could involve not just breaking up companies but also implementing more robust regulations that promote transparency, fair competition, and consumer protection. Additionally, fostering a global consensus on how to handle these tech giants will be crucial, given their international reach and influence. Regardless of the specifics, the era of unchecked dominance by a few tech companies is coming to an end, opening a new chapter in the digital economy's evolution.

Online Gaming and Betting Laws

SECTION 2

THE US SENATE PASSES THE KIDS ONLINE SAFETY ACT ("KOSA") TO REGULATE MINORS AND ONLINE ACTIVITIES

NEWS

KOSA, as it is widely known, plans to create a "duty of care" for intermediaries and online gaming platforms to ensure adding design features that protect minors from accessing "inappropriate" and "harmful" content. Passed by the US Senate, the bill's future is still uncertain as widespread protests are ongoing against the bill's enactment.

LEGAL TALK

Alternately titled KOSPA which is a modern form of the Children's Online Privacy Protection Act of 1998 and the Kids Online Safety Act of 2024, the bill seeks to hold the "big tech" liable and to provide minors with options to protect their information, disable addictive product features, especially related to online gaming and gambling sites, and opt out of personalised algorithmic recommendations. In the specific context of online gaming and betting sites, the bill is touted as one of the most comprehensive bills made to safeguard minors and their online footprint. Some of the provisions of the bill include measures to limit the typical tactics used by gaming sites to lure in minors, such as "rewards based on time spent on platforms," "automatic playing of media," and "other notifications." Tracking the "geolocation of the minors" and restricting the ability of other players to communicate with these kids through online chat rooms is also another proactive measure the bill aims to implement (Sec 4). This could mean that under Section 2(10) of the act, which defines "online games," sites must ensure age-gating features, enhanced age verification processes, and potentially limiting or altering content that might be deemed harmful to minors, including restricting financial transactions within the game. When it comes to gambling and betting sites, the act aims to give intermediaries a "duty of care" in terms of promoting, advertising, and marketing gambling to minors. However, despite the presence of such "beneficial provisions," the bill might not live long enough to see itself turn into legislation as there are widespread protests against the same.

THE WAY FORWARD

The bill is not the magical remedy to all the present problems, as it needs to include many pertinent points raised by the critics and whistleblowers and placate the anxieties of the tech companies. As the bill moves into the House of Representatives for the next stage of voting and debating, one can hope that these recommendations will be added and the act can be a model for other countries to replicate.

PROVIDING INTELLECTUAL RIGHTS PROTECTION TO ONLINE GAMES IN INDIA

NEWS

The e-gaming industry in India has witnessed a rapid expansion of 28% compound annual growth rate ('CAGR') between FY20 and FY23. There have also been projections which indicate growth to ₹33,243 crore by FY28, with a sustained 15% CAGR. With this rapid expansion in the gaming industry, there is an alarming need for advanced measures to protect intellectual property ('IP') rights within the online gaming sector. The world of online gaming is an ever-evolving world full of innovations and imagination. Intellectual Property Rights form a vital cornerstone in the gaming industry, ensuring the protection of everything we hold dear, from cherished characters to the innovative technologies that create immersive gaming experiences. IPR protection to online games has been a critical issue in India for a long time. The industry witnesses continuous advancements in technology and other significant software developments. This makes it even more vital to protect the intellectual components in the e-gaming sector.

CURRENT CHALLENGES IN THE LEGISLATIVE PROTECTION

In India, there is no specific regulation governing the gaming industry, and as a result, video games are not classified under any particular category of IP Law. However, the existing legal frameworks offer hypothetical protection for e-Sports in the country. For instance, the Copyright Law covers the background music, game source code, and other artistic elements of e-Sports. Trademark Law safeguards the names of e-Sports, unique character identifiers, and symbols. Similarly, Patent Law provides protection for gaming equipment, such as consoles, joysticks, and other technical devices that facilitate gameplay. Trade secret laws also play a role when game producers or creators choose not to disclose their codification.Despite these laws exists, the gaming industry faces significant threats in various forms.

GAME CLONING

One of the major challenges in protecting intellectual property (IP) in online gaming is the issue of game cloning. It happens when a company replicates another company's game and markets it as its own. This not only infringes on the original game's IP but can also damage the reputation of the original game and its developers. Game cloning is especially common in the mobile gaming industry, where low entry barriers and easy access to development tools make it straightforward for companies to copy popular games. Such cloning can confuse consumers, leading to lost revenue for the original developers. It can also tarnish the reputation of the original game, sometimes resulting in negative reviews and lower ratings, which further hurt its business performance and success.

DIGITAL PIRACY

The digital nature of online games also facilitates piracy, which allows users to easily share and distribute illegal copies. Digital games can be easily obtained and shared illegally, leading to lost revenue for the game's creators. This issue is especially troublesome for smaller developers who often lack the resources to implement effective anti-piracy measures. Some companies have tried using digital rights management **(DRM)** technology to combat piracy, but this approach can make games less accessible to legitimate users and may cause technical problems. As a result, piracy remains a major concern in the industry, particularly for those with limited means to protect their creations.

COPYRIGHT IN THE LIVE STREAMING OF VIDEO GAMES

The absence of legislation and the uncertainty surrounding potential copyright issues related to livestreaming video games, is particularly concerning for content creators and streamers. They may unknowingly infringe on copyright when using game material in their live streams. It is also uncertain whether a video game would qualify as a "cinematograph film" under the Copyright Act. Section 2(f) defines a cinematograph film as "*...any work of visual recording produced through a process from which a moving image may be, and includes a sound recording accompanying such visual recording, and 'cinematograph' shall be construed as including any work produced by any process analogous to cinematography, including video films...*" While video games could be interpreted as cinematograph films due to the reference to a "process analogous to cinematography," the lack of relevant precedent in India leaves this question unresolved. The *Mattel Inc. and Ors. v. Jayant Agarwalla* case perfectly describes the issue of copyright protection of the game 'Scrabble' in India. Mattel, owning the 'Scrabble' trademark globally (excluding the USA and Canada), claimed copyright protection for the game's layout and rules as an artistic work under the International Copyright Order, 1991. They accused the defendants, creators of a similar online game 'Scrabulous' of infringement by using deceptive metatags and copying design elements. However, the court ruled against copyright protection, citing the doctrine of merger and Section 15(2) of the Indian Copyright Act, which states that when the idea and expression cannot be separated, copyright does not apply. Despite this, the defendants were prohibited from infringing the 'Scrabble' trademark, emphasising the importance of trademark protection in such disputes. The Indian judiciary has not explicitly extended protection to video games, but the case of *Sony Computer Entertainment Europe Ltd. v. Harmeet Singh and Ors.* is the most relevant case addressing copyright issues in video games. In this case, the Delhi High Court issued an interim injunction against the defendants for modifying PlayStation consoles to run pirated video games, which they were distributing.

LACK OF GAMING PATENTABILITY

Under the Indian patent law, the “mere” act of playing a game is not considered an invention. As a result, games, along with the specific technologies or techniques they incorporate, are not eligible for patent protection. While innovations that combine software with hardware may be patentable, purely software-based gaming mechanics often do not qualify for patent protection. This limitation restricts developers from safeguarding unique game mechanics and features, leaving them vulnerable to imitation. Another issue is that gaming companies often use player names, photos, jersey numbers, and other identifiers within the game or for promotional and advertising purposes, which may infringe upon the owner's exclusive rights. The enforcement is further complicated by the digital nature of gaming and jurisdictional issues, making it difficult to effectively safeguard and uphold these rights.

CONCLUSION

The online gaming industry in India has been constantly on the rise due to increase in digital accessibility. At this stage protecting the intellectual property rights in the game industry becomes increasingly vital. By addressing the current legislative lacunas and subsequently fostering a protective environment for developers, India can enhance its position in the global gaming market. The country’s legislation needs to ensure that creators and developers are adequately rewarded for their innovations. The future of gaming in the country is reliant on the effective protection of intellectual rights, which is the fundamental driver of growth and creativity in this dynamic sector. Apart from legislative protection, game inventors, developers, or owners should also prioritise robust, comprehensive protection of their game rather than relying only on fragmented measures that safeguard individual components. Protecting a game's intellectual property is an important first step, but to truly safeguard the game and support its creators, the owner should also actively pursue legal action against violators. The need today is to develop innovative strategies in the technological field itself to effectively enforce these rights. Wealthy game owners can establish an online investigative team to monitor competing games while small developers might consider outsourcing this task to specialised firms, as this can be cost-effective while still yielding strong results.

FinTech

SECTION 3

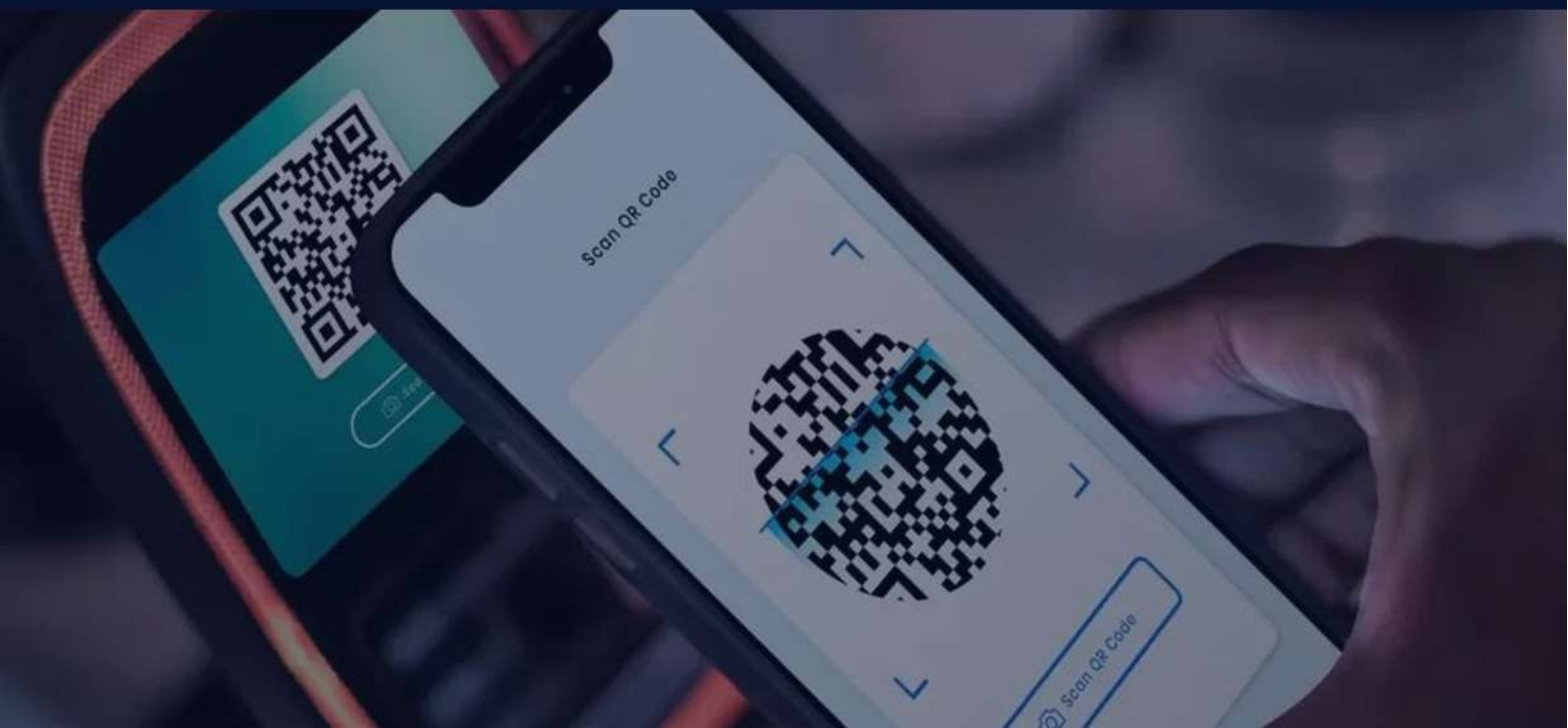
RESERVE BANK OF INDIA ("RBI") ISSUES DRAFT RULES ON THE DUE DILIGENCE TO BE CARRIED OUT FOR AADHAR ENABLED PAYMENT SYSTEM ("AEPS") TOUCHPOINT OPERATORS

NEWS

The RBI recently released its Draft Directions on Aadhaar Enabled Payment System – Due Diligence of AePS Touchpoint Operators. The RBI's draft directions aim to prevent fraud by streamlining the onboarding process for AePS touchpoint operators and requiring ongoing due diligence by banks.

LEGAL TALK

AePS refers to a payment system run by the National Payment Corporation of India ("**NPCI**") that facilitates interoperable financial transactions through the Business Correspondent ("**BC**") or the AePS touchpoint operators of any bank, using Aadhaar authentication. These operators typically act as intermediaries between the bank and the customer, providing services like cash deposits, withdrawals, balance inquiries, and fund transfers in remote or underserved areas. One major problem, however, is the lack of two-factor authentication in the system which has led to multiple incidents of financial fraud, where fraudsters exploit compromised Aadhaar numbers or illegally obtain biometric data. To protect users from these threats, the RBI is now implementing concrete measures, like the newly issued guidelines, to curb such fraudulent activities. The directions mandate that due diligence by the acquiring banks is carried out by all AePS touchpoint operators onboarded by it, as per the Customer Due Diligence procedure laid out in RBI's master directions on KYC, 2016. In cases where an operator has not carried out any transactions for a continuous period of six months, the onboarding bank must carry out the requisite updation of KYCs. Banks are also mandated to monitor the activities of their touchpoint operators, set transaction limits, and periodically verify that transactions align with the operator's location and risk profile. This rigorous onboarding procedure and surveillance intends to prevent fraudulent operators from entering the system and to ensure that those already onboarded are continuously monitored and reassessed. This is crucial for early detection of unusual activity. Additionally, the NPCI and acquiring banks must ensure that a particular touchpoint operator is only onboarded by one such bank. Restricting operators from onboarding multiple banks, reduces the risk of them escaping scrutiny by being associated with multiple institutions.



In line with the Draft Framework On Alternative Authentication Mechanisms For Digital Payments, the regulatory body aims to enhance digital transaction security, including AePS, by introducing alternative methods of Additional Factor Authentication ("**AFA**"). One of the authentication factors must be "dynamically created," meaning it is generated after the payment initiation, making it unique and non-reusable. It must also be ensured that both factors of authentication are of different kinds, such as passwords, PINs, and software tokens. Issuers are allowed to apply a risk-based approach when determining the appropriate AFA for a transaction, considering the user's risk profile, transaction value etc. This discretion allows them to enforce stricter controls where required, without burdening low risk transactions. They must also implement near real-time alerts for transactions and obtain explicit customer consent before enabling new AFAs, ensuring the robustness and integrity of the authentication process.

THE WAY FORWARD

By enforcing ongoing due diligence, monitoring, and setting tailored transaction limits based on risk profiles, the RBI is proactively mitigating potential fraud. The emphasis on robust cybersecurity, along with efforts to increase customer awareness, are commendable initiatives to enhance security against online fraud. If effectively implemented, these measures could significantly boost trust and security in AePS and digital payment systems in India, benefiting all kinds of users and helping reach its primary goal of financial inclusion. However, their success rests on strict enforcement by banks and NPCI, as well as the ability to quickly adapt to new threats in the digital landscape.

NATIONAL PAYMENTS CORPORATION OF INDIA INTRODUCES DELEGATED PAYMENT MECHANISM FOR SECONDARY USERS THROUGH UPI

NEWS

UPI has emerged as a popular mode of payment with a humongous user base of around 200 million individuals in India. However, National Payments Corporation of India ("NPCI") foresees further potential for expanding the user base to include secondary users such as minors and senior citizens. In its release, NPCI announced that it is set to launch 'UPI Circle', which users can delegate to their trusted secondary users to make payments.

LEGAL TALK

NPCI has introduced 'UPI Circle' to address the unmet needs of users without bank accounts. This has been unveiled in two categories – full delegation and partial delegation. Full delegation allows secondary users to both initiate and complete transactions, whereas partial delegation allows users to initiate a transaction, but the primary user has to complete the transaction with the UPI pin. However, this poses a risk for potential misuse as the targeted individuals, including minors and elderly citizens, are more vulnerable to financial fraud. RBI released a statement on its developmental and regulatory policies, proposing that this feature will allow an individual (primary user) to set a UPI transaction limit for another individual (secondary user) on the primary user's bank account. To prevent misuse, NPCI has issued guidelines for members to adhere to. These guidelines provide users with a choice of UPI app and the option for full or partial delegation. Primary users can link with secondary users by scanning their QR code and selecting their number from the contact list. Manual entry of mobile numbers is restricted to prevent scams. Up to 5 secondary users can be added. However, a secondary user can only accept a delegation from one primary user. All secondary users must authenticate using the app passcode or biometrics. There is a maximum usage limit of Rs. 15000 per month and a maximum per transaction limit of Rs. 5000 for full delegation. RBI guidelines for 'Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems' have been reemphasised by NPCI for resolution of customer complaints.

THE WAY FORWARD

The UPI Circle feature is valuable for individuals who may not have the capacity or desire to manage their digital transactions independently but still wish to access and benefit from such financial services. This initiative allows multiple members of a family to use a single bank account for UPI payments, which could significantly boost the adoption of digital payments method in rural areas where families often share one bank account. While it is a move towards financial inclusion, there is an added onus on the users to limit access and impose strict controls on the extent of delegation. As the regulatory body, RBI is expected to issue detailed instructions on using delegated payments through UPI as prescribed under the Payment And Settlement Systems Act, 2007. These guidelines could emphasise its regulation by the Payment Service Providers and UPI apps. Primary users should be presented with flexible options for setting transaction limits. Moreover, RBI's draft framework on alternative authentication mechanisms for digital payment transactions could also be consequential in enhancing security measures in digital transactions.

RESERVE BANK OF INDIA ('RBI') TIGHTENS NORMS FOR NON-BANKING FINANCIAL COMPANY - PEER TO PEER LENDING PLATFORMS ('NBFC-P2P')

NEWS

Recently, the RBI released directions for NBFC-P2P ('**Amended Provisions**'). The RBI tightened the norms to curb certain practices adopted by NBFC-P2P platforms such as violation of the prescribe funds transfer mechanism, promoting P2P lending as an investment product with features like tenure linked assurance minimum returns etc. these directions have been released by RBI by amending the previous Master Direction - NBFC P2P (Reserve Bank) Directions, 2017 ('**Existing Provisions**').

LEGAL TALK

According to paragraphs 4(1)(v) and 4(1)(vi) of the existing provisions, NBFC-P2P means an NBFC which acts as an intermediary providing the services of loan facilitation via online medium or otherwise. Following changes have been made in the amended provision:

- Under the existing provisions, an NBFC-P2P shall not cross-sell any product except for loan specific insurance products. The amended provisions also add that they should also not cross sell any insurance product which is in the nature of credit enhancement or credit guarantee. By clarifying permissible practices the amendments aim to ensure that P2P platforms focus on their core lending function and provide a transparent consumer experience.

- The existing provisions required NBFC-P2P to disclose to the lender details about the borrower including personal identity, required amount, and interest rate sought and credit score as received by the NBFC-P2P. Under the amended directions, an NBFC-P2P has to disclose the borrower's consent as well which should be kept on record. This change is designed to enhance the trust of the borrowers and ensure that they are aware and have agreed to share the information. It also aligns with broader data protection principles.

- The amended provisions mandate NBFC-P2P to disclose on their website, the losses borne by the lenders on principal and interest. The existing directions required them to disclose only its portfolio

- performance, including share of non-performing assets on a monthly basis and segregation by age. The objective of this amendment is to enhance transparency and help in informed decision-making by providing lenders with a clear picture of actual financial impacts and risks associated with their investments.

- Under the amended provisions for NBFC-P2Ps, there is a new restriction on outsourcing the pricing of services and fees charged to borrowers and lenders, which was not explicitly addressed in the previous regulations. While NBFC-P2Ps are still prohibited from outsourcing core management functions such as internal audit, strategic and compliance functions, and decision-making functions related to KYC compliance, the updated guidelines now specifically include the pricing of services/fees as a function which cannot be outsourced. By retaining pricing as an internal function, the NBFC-P2P can maintain better oversight and ensure that the fees are fair and transparent.

- The amended provisions have also mandated that the NBFC-P2P shall explicitly mention its name (as mentioned in the Certificate of Registration) along with its brand name in all promotional material and in communication with stakeholders.

THE WAY FORWARD

These changes are expected to lead to enhanced transparency and accountability and reflect a consumer-oriented approach. By requiring greater disclosure, obtaining explicit consent, and limiting certain outsourcing activities, the changes aim to build trust, improve data protection, and prevent potential conflicts of interest. However, such additional requirements may add some administrative burden on NBFC-P2P platforms and may hinder their flexibility or cost efficiencies.

ARTIFICIAL INTELLIGENCE

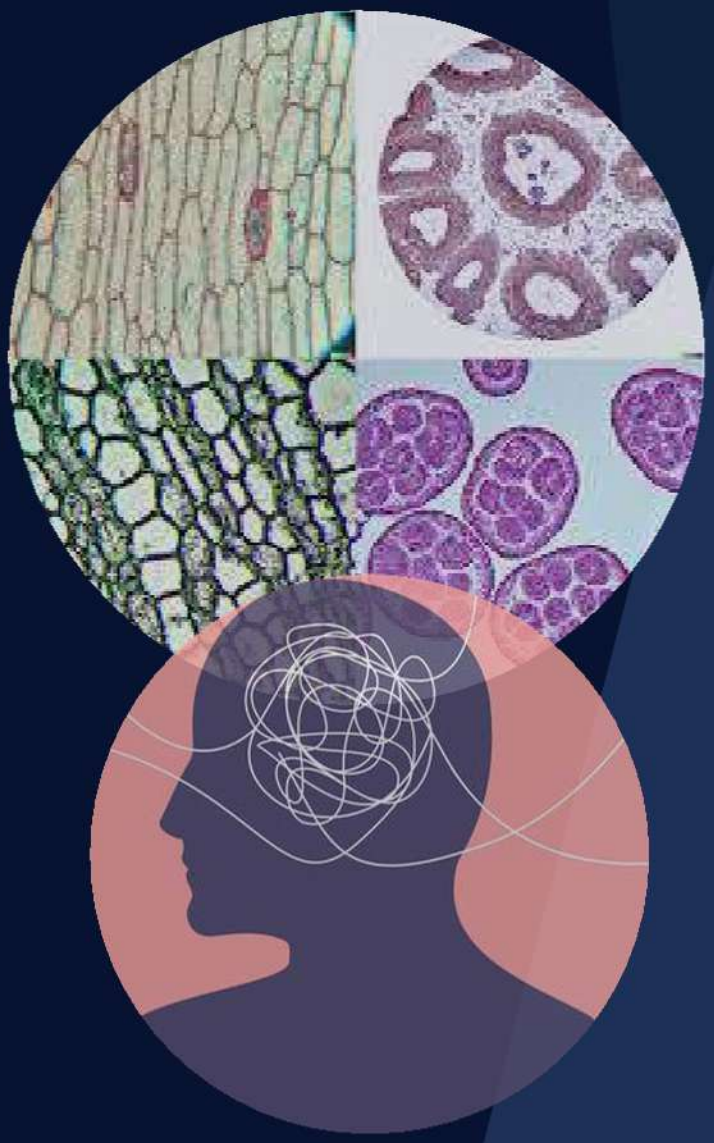
SECTION 4

FLOOD OF 'JUNK': HOW AI IS CHANGING SCIENTIFIC PUBLISHING

NEWS

AI generated text and images are causing a stir in the scientific research industry. While AI has indeed made the task of scientific researchers easier, there has been an influx of instances in the form of false data, bizarre images, graphs and plagiarism of work which has compelled publishers to retract the study that they publish within a short period of time, seriously affecting the integrity of scientific research and causing serious research misconduct.

LEGAL TALK



Research misconduct, particularly involving fabrication, falsification and plagiarism abbreviated as FFP is an international concern as it poses a threat to the rectitude, reliability and objectivity of research. While AI has become a valuable tool for researchers, aiding in tasks such as summarising data and information, language translation, image generation, and providing briefs of articles, it has also contributed to the rise of publications with flawed, inaccurate, or plagiarised content. These 'junk papers' have sometimes bypassed peer review, leading to an increase in retractions. The 'Society for Scientific Values', an independent organisation investigates scientific misconduct although India does not yet have a governmental authority to handle such cases as the US does with its 'Office of Research Integrity'. However, various existing laws can be invoked to address such issues. 'Negligence' under tort law is defined as the violation of a duty resulting from the failure to take action that a wise and a reasonable man would not do, guided by the principles that typically govern human affairs. It can be asserted when the researcher is aware that he/she has employed the help of AI tools to aid in their research and has not shown a duty of care to oversee the AI's output which led to the publication of false data, text or images. Under this, the researcher and publisher are liable as an AI tool requires an input or prompt to provide any kind of results, thus holding the AI developer responsible for negligence is unfair as it is expected from the

researcher to proof read or ensure the correctness of information provided by the AI bot before he/she includes such information in their study which would be read and relied upon by so many people from the scientific research community.

'Intellectual property laws' can be invoked when the researcher has plagiarised and rephrased an author's work to avoid getting caught by the peer review process. Section 51 of the Copyright Act deals with infringing copies of literary works. Thus the plagiarised work of another author that gets published elsewhere would come under the domain of this section. At the same time, plagiarism to an extent or a set percentage is considered fair use but if it is beyond the set limit, the researcher ought to compensate the original author. Contractual obligations arise when research is funded by the government. If AI-generated false information is published and causes harm to society or fellow scientists who rely on the research, the researcher may be held liable under the 'Indian Contract Act' under fraud or misrepresentation or both, say for e.g. A researcher uses an AI tool to generate data for a government-funded study on renewable energy. The AI produces data with inaccuracies, but the researcher knowingly submits this flawed data as accurate and complete in their final report. The researcher presenting inaccurate data and deceiving the government into believing the research is valid can render him liable for fraud.

Another interesting way to hold such researchers liable for research misconduct would be under Section 51 of the BNS. This section sheds light on the liability of the abettor when the act he abetted was not done but a different act was performed, in such cases the abettor would be held liable for the different act done in the same way as if that was the act he intended to abet from the beginning. Under this section, the researchers would be considered to be the abettors and the person doing the different act would be the AI tool. Regardless of what the AI tool generated, the liability would fall on the researcher as if they were the ones that abetted the act, even if the act they intended to abet was something else and something else was committed. For e.g., A researcher is working on a government-funded project to develop and validate a new COVID-19 vaccine. The researcher uses an AI tool to analyse clinical trial data, including patient immune responses and side effects. The AI is supposed to identify the vaccine's efficacy and any potential adverse reactions. Due to an error in the AI's programming or data interpretation, it incorrectly analyses the trial data, significantly underreporting the frequency of serious side effects such as severe allergic reactions. The researcher notices the AI's analysis seems unusually optimistic but

eager to publish positive results and under pressure to deliver, proceeds to submit the AI-generated report without further validation. The study is published, and based on these results, the vaccine is approved for widespread emergency use. The vaccine is then distributed to the public. Individuals receiving the vaccine may suffer from the allergic reactions that were not disclosed. The vaccine's deployment could lead to public health crises, loss of life, and a significant loss of public trust. These were just a few legal frameworks that could help curb the menace of research misconduct and hold the researchers liable for their deeds.

THE WAY FORWARD

Research misconduct being a problem of global concern must be defined uniformly and needs a standardised approach. With the rise of AI in scientific research, several key measures are essential. Researchers must educate the public and scientific community about their AI tools, including their operation, justification, and potential biases. They are responsible for identifying and addressing faults in these tools. Additionally, researchers should clearly define and explain synthetic data and its use to avoid issues with plagiarism or misinformation. Transparency about the AI tools used, including technical details, is crucial for trustworthiness, Generative AI tools that store data should be avoided to protect sensitive information,and AI tools should not be listed as authors. Finally, a dedicated legislative body should be established to recommend, investigate, and enforce standards for scientific misconduct.

"CELEBRITY" STATUS IN PERSONALITY RIGHTS : A CASE OF CONTRAST BETWEEN INDIA AND AMERICA

NEWS

In a recent judicial development that can prove to be pivotal for AI Businesses as well as Individual personality rights in India, the Bombay High Court in the case of *Arijit Singh vs Codible Ventures LLP and Ors.*, passed an ex-parte interim order against a number of defendants, including AI Platforms, for unauthorised use of the artist's personality traits. The judgement talked about the importance of personality rights for celebrities and establishes essentials for an action to protect these rights. The judgement also talks about the importance of these rights in the AI regime and establishes limits of AI use. Further, in a similar development, recently a group of Bi-partisan senators in the USA introduced the Nurture Originals, Foster Art, and Keep Entertainment Safe Act of 2024, popularly known as the NO FAKES Act. The Act primarily protects personality rights of all individuals and confers those with the status of property rights, with features like assignability and inheritance attached to them.

LEGAL TALK

In India, personality rights are an emerging part of the copyrights bundle. Personality rights broadly include the Plaintiff's name, voice, photograph / caricature, image, likeness, persona, and other attributes of his personality. Such rights, while not emanating from any statutory position, have been acknowledged in a plethora of judicial decisions. These rights are a branch of publicity rights that are borne out of the constitutional rights of Privacy. In India the sudden emergence of multiple disputes owing to non-authorized usage of marketable personality traits of celebrities evidence the current importance of personality rights, especially in the context of AI businesses. In a series of latest litigations instituted by celebrities ranging from Jackie Shroff, Karan Johar to Anil Kapoor, it looks like the time for accountability is here. In the immediate case, the plaintiff brought action against multiple defendants, who by multiple means infringed his personality rights, primarily being AI apps which provided his voice emulator. The judgement lays out this suggests a test of qualification for protection of personality rights, wherein, establishing a celebrity status for the plaintiff is only the primary ingredient, which has to be followed up by identifiability of the personality traits from the

The judgement lays out this suggests a test of qualification for protection of personality rights, wherein, establishing a celebrity status for the plaintiff is only the primary ingredient, which has to be followed up by identifiability of the personality traits from the usage in question, and if all this was done without any authority derived from the Right-holder. While the judgement is a welcome step in light of the growing developments in AI technologies and usage in India, concerns arise around the lack of advancement in perspective with the pace of technological growth. The judgement provides protection to personality rights but also adds a filter of "celebrity" to be qualified for such protection. This undefined pre-requisite of "celebrity" status in the light of the pervasive casual imitation of personality elements all over social media is a major concern. The judicial history of this prerequisite can be traced down to the 2015 judgement of *Shivaji Rao Gaikwad vs M/S.Varsha Productions*, where the Madras High Court premised the celebrity status in the identification of the personality traits from the usage in question. That case, as well as many other cases concerning personality rights, were primarily concerned with the usage of popular names, like "Rajnikanth", "Karan Johar" and "Anil Kapoor". However, with the emerging technology, infringement of personality rights is not solely limited to the usage of pre-established identity but also extends to the deceptive usage of physical characteristics. The judgement itself talks about the ill effects of unauthorised AI-generated content and how the consequences are not just limited to economic harms, but also extend to potential misutilisation of these tools in other ways. Even after this, the court failed to consider how future litigations would fail at the first step itself when countered with the lack of "celebrity" status, even when personality traits are identifiable from the usage in question. The court must recognize that the earlier judgements established celebrity status out of the identifiability of the personality traits and not the long illustrative history of the person's achievements and professional endeavours that the High Court has considered in the immediate case. This new approach is very harmful for the common person whose identifiable personality traits can be used to create manipulative content.

CONTRAST WITH THE 'NO FAKES' ACT

The NO FAKES Act has been designed to protect all individuals, section 2 (a) (2) of the act defines "Individual" as a human being, living or dead. The section 2 (a) (5) of the act defines "Right holder" as the individual whose voice or visual likeness is at issue with respect to a digital replica and any other licensee or authorised individual. This is a conscious development in the USA, where earlier personality rights were recognized by some states only for public figures and/or celebrities. The congress recognized that the capabilities of generative AI empower it to easily imitate the personality traits of virtually anyone. This has to be looked into in the light of both social and economic factors. Multiple different personalities hold influence over multiple different sectors in modern times. Just like it is deceptive to use the personalities of actors in commercials, it can very well be effective to use the personality traits of the SEBI chief to spread financial misinformation. The question to be asked is what criteria would then decide the "celebrity" status of the person involved? Further, In the age of the growing content economy, with new age micro celebrities emerging every day, who base all of their livelihood on personality, what would be the criterion to adjudicate their "celebrity" status?

THE WAY FORWARD

The Bombay High Court in recent times has emerged as the harbinger of justice for the media industry as it tackles with emerging technology and infringement of age-old fundamentals of law. Following this regime of celebrity exclusive personality rights can be detrimental to all future litigations where personality rights of normal people are breached by the unregulated AI regime and multiple other avenues. Hope can be placed in the honourable High Court to understand this lacuna and rectify it. Further, in the light of multiple emerging issues concerning violation of personality rights due to AI service providers that enable access to tools that have a potential to recreate personality traits, it is now a legislative imperative to provide statutory identification to these rights. India has to follow the lead of multiple other nations which have implemented such statutes, a recent one being the NO FAKES Act of USA. Further, much-anticipated AI legislation is also needed in India to regulate the emerging AI industry in India, which has displayed a blatant disregard of established legal norms.

DATA PRIVACY

SECTION 5

USER VERIFICATION IN SOCIAL MEDIA PLATFORMS

INTRODUCTION

Policymakers are increasingly concerned about online harms caused by anonymous users and fake profiles. To address this, governments worldwide are considering mandatory online user verification to confirm identities of perpetrators and ensure they are who they claim to be. As mandatory verification becomes more common, it's crucial to consider how extensively these requirements should apply to social media platforms in India. Policymakers face the challenge of balancing citizens' freedom with national security, while also ensuring that digital innovation in India isn't hindered.

ONLINE VERIFICATION

Online verification can occur through various methods, ranging from simple captchas to full identity checks. Verification relies on "identifiers," such as names, dates of birth, or IP addresses, which distinguish individuals. Most online platforms automatically collect metadata, like IP addresses and cookies, which describe and track user activity. 'Identification' involves self-reported information, like a name, without third-party validation. 'Verification/Authentication' confirms this information's accuracy using documents or unique identifiers, like Aadhaar numbers. While simple identification is easy and common, it doesn't confirm the information's validity, potentially allowing anonymous profiles to exist. Authentication, however, significantly reduces anonymity, as additional identifiable information is required. For instance, using social media might only need an email, while online banking demands more details like location and mobile number, further eroding anonymity. Therefore, verification requirements should limit the reduction of anonymity to what's necessary for their purpose, using basic identification when sufficient and full verification when needed.

METHODS

Having clarified the difference between identification and verification, let's now look at various methods to achieve these purposes, specifically those prominent in India. Statistical data shows that most leading social media companies ask for a User Name, a valid email address and a telephone number. The information is crucial for customer onboarding and account verification. Some apps such as dating sites could also ask for the DOB. Methods like Know Your Customer norms have not been discussed here due to their obscurity in social media platforms.

1. OTP System:

Phone numbers are widely used for authentication, with One-Time Passwords ('**OTPs**') sent to verify users. Two-factor authentication ('**2FA**') adds an extra layer of security by requiring users to confirm their identity in two steps—typically by entering a password and then an OTP sent to their phone or email. Some platforms use security questions or send verification links as the second step. However, 2FA isn't foolproof. Phishing attacks can trick users into revealing OTPs, and SIM swapping can allow attackers to intercept OTPs sent to phones. Additionally, if a user's email or phone number is compromised, the security of the entire account is at risk.

2. Data Collection & Preservation

The secondary method of identity verification focuses on what platforms can do independently to trace the origin of content, rather than on direct user verification. Significant Social Media Intermediaries ('**SSMIs**'), as defined under the Information TeInformation Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('**IT Rules**') are required to identify the first originator of content when ordered by a court or competent authority under Rule 4 of the IT Act. However, the rules do not prescribe a specific mechanism for this identification, leaving platforms like WhatsApp responsible for developing their own solutions. Enabling traceability could weaken encryption, making users more vulnerable to malicious attacks. If the originator is outside India, the first recipient in the country is deemed the originator, allowing evasion through foreign numbers. Current technology only identifies phone numbers or email addresses, not actual individuals, and platforms can only trace origins within their own network, missing cross-posted content. This means that identifying the absolute originator of content is nearly impossible without breaking encryption, which would negatively impact all users.

Under Section 9 of the Digital Personal Data Protection Act ('**DPDPA**'), obtaining verifiable consent from a parent or lawful guardian is required if a minor's data is processed. This requires data fiduciaries to verify the age of the claimed parent, their relationship with the child, and the parent's identity. To comply, platforms may need to authenticate documents, effectively necessitating the verification of all users' identities and ages. This contradicts the principle of data minimization and poses cybersecurity risks by necessitating the storage of vast personal data. The government's consideration of using electronic tokens via systems like DigiLocker adds complexity. This reliance on electronic and government-authorised verification may not address the needs of individuals in remote areas with limited digital infrastructure, potentially leading to exclusion or inaccurate verification. Social media platforms will need to develop the technical infrastructure for this verification while ensuring data security - something which smaller sites might not be able to fund, hindering competition and innovation.

Less invasive, ex-ante alternatives to current methods can be considered to prevent online harms. Instead of focusing solely on identifying and punishing offenders after the fact, we should explore proactive measures. For instance, internet platforms automatically collect metadata like IP addresses, which law enforcement can use to determine the network provider and general location without exposing the user's identity. While this approach is more effective after a crime is committed, such as identifying perpetrators, it may not work for platforms requiring upfront user verification, like dating sites. Nevertheless, it's a viable option for other contexts. The state must justify any privacy infringements by proving they bring more benefits than harms.

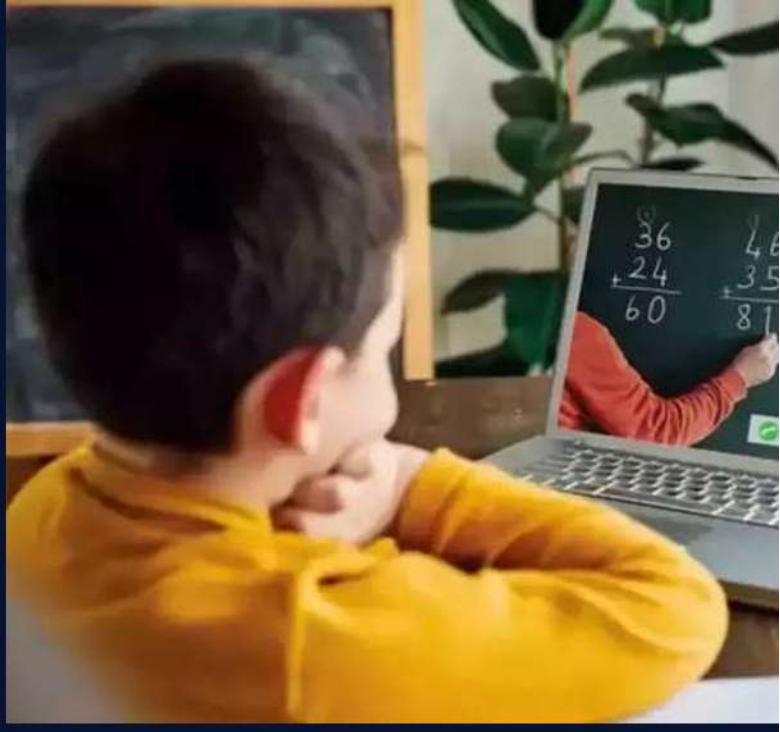
OTHER COUNTRIES

South Korea introduced an 'internet real-name system' as a part of an amendment to the Public Official Election Act in 2004, requiring users to verify their identities before commenting on news sites during elections. However, later the Constitutional Court ruled it unconstitutional, citing violations of free speech and personal identity. The Court also found no evidence that the policy reduced online harms and noted that it led to increased hacking incidents due to the accumulation of vast amounts of user data. In 2020, Brazil's Senate approved a "Fake News Bill" requiring mandatory identification through National ID and mobile numbers for social media and messaging services. Due to privacy concerns, the draft was revised to make identification non-mandatory. The UK does not have a real name policy, introduced an age-gating requirement with the Online Safety Act ('OSA') in October 2023. The OSA mandates that online platforms ensure children do not access harmful content through age assurance, but does not specify how this should be done. Concerns have been raised about the impact on free speech and privacy, as platforms may either heavily moderate content or require all users to verify their age, increasing data security risks. These varied approaches indicate a broader trend where countries are increasingly aware of the limitations and potential pitfalls of rigid user verification policies. It's clear that implementing mandates like these does not *guarantee* a lower crime rate and sometimes may even have adversarial implications. Concerns related to privacy of personal identity has led these countries to revise the law and try to look for alternates. This demonstrates that effective online regulation requires a nuanced understanding of the balance between security, privacy, and freedom. Nations need to learn from each other's experiences, adapting their strategies to address specific contexts and concerns while striving to protect users from online harms without compromising fundamental rights. This global perspective suggests that instead of adopting blanket mandates India, too, must focus on creating flexible solutions while safeguarding privacy and ensuring inclusivity. Let's look at the pitfalls of such an approach.

THE WAY FORWARD

Justice Chandrachud, in the 2017 Puttaswamy case, referenced Alan Westin's theory of privacy, recognizing anonymity as a key aspect, enabling individuals to remain unidentified in public spaces. Anonymity is crucial for free expression, dissent, and protecting vulnerable groups, especially in restrictive environments. Safeguarding the data of millions of users is also a humongous task. With 759 million active internet users in India, the process would require substantial investment in infrastructure, manpower, and data security, driving up costs and potentially excluding smaller players from the market. For marginalised communities without valid identification, mandatory verification could create access barriers, further alienating them and hindering their participation online. This approach could also undermine India's Digital India mission, which aims to create a more inclusive digital society and economy. User verification can't be one-size-fits-all. Each service needs a tailored approach considering its nature, risks, and privacy concerns. Social media platforms, unlike the financial sector, face bigger trade-offs with strict verification, potentially infringing on fundamental rights. India must weigh these complexities and develop proportionate, balanced solutions.

FORMULATING MECHANISMS FOR OBTAINING VERIFIABLE PARENTAL CONSENT UNDER DPDPA WILL LIKELY BE UP TO THE COMPANIES



NEWS

The IT Ministry is likely to step back from prescribing any specific technological measure for tech companies to gather verifiable consent from parents in order to establish the relationship between children and their parents. This essentially means that it will be up to the discretion of the companies on how they want to seek such consent under the upcoming data protection rules.

LEGAL TALK

According to the Digital Personal Data Protection Act ('DPDPA'), a 'child' is someone who has not attained eighteen years of age. Section 9(1) of the DPDPA requires data fiduciaries to obtain verifiable parental consent before processing any personal data of a child or a person with disability. Simply put, such verification should be done prior to a child using an online service. The act in itself does not mention anything about the procedure for obtaining such consent, and the industry is in a fix over formulating a compliance mechanism. In the absence of any specific guidelines from the government on the same, tech companies would have to rely on global privacy laws with similar provisions. The General Data Protection Regulation ('**GDPR**') for example, requires data controllers to make 'reasonable efforts' to verify that the consent provided on behalf of a child below thirteen years of age, is provided by the parent. Further, the United States Children's Online Privacy Protection Act ('COPPA') creates a mandate for a 'reasonably designed' method to be chosen by operators. It additionally prescribes certain consent methods such as signing a consent form and sending it back electronically; using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; connecting to trained personnel via a video conference; or verifying a picture of a driver's licence or other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology, among others. 'Reasonable efforts' is understood to mean that the law will evaluate whether a data collector has taken reasonable steps to confirm that a person is of age to consent to data collection, considering the risks involved and the current technology, in case of a complaint. While DPDPA does not mention reasonable efforts, section 9(5) requires a Data Fiduciary to process personal data of children 'in a manner that is verifiably safe' to obtain notification of exemption from the obligations under the section, subject to the government's satisfaction. There is limited to no clarity on what course of action will be taken in case of complaint alleging violation of Section 9 and how the government will determine whether the Data Fiduciary made 'reasonable efforts' to obtain verifiable consent. The rules must provide complete clarity on the same, as in an alternative scenario, Section 9 will be a glaring loophole in the act which can either be used by the Data Fiduciaries to escape liability or by the government to impose liability rampantly.

THE WAY FORWARD

Processing of personal data relating to children while maintaining privacy compliances can be a hard nut to crack. The tech industry is faced with key challenges such as age-based content filtering, processing of sensitive personal data, due diligence for companies that process child personal data for ancillary services, establishment of authentic guardianship relationships, compliance costs, etc. As we await the DPDPA rules anxiously, it is essential for tech companies, especially those that process large scale personal data, to devise mechanisms for compliance according to global standards.

CONTRIBUTORS

WRITERS

SATVIK MITTAL
PRATYUSH SINGH
ANJALI PANDE
KALYANI KIRAN
ANANYA SONAKIYA
ARUNIMA RAMAN
SOUVICK SAHA
LAVANYA CHETWANI
BHAVYA BHASKAR
ALOK SINGH MOURYA
TRISHNA AGRAWALLA
ANUSHKA GUHA

EDITORS

HARSH MITTAL
LAVANYA CHETWANI

DESIGNERS

SAMRIDHI BAJORIA
TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL