LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

DECEMBER 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्ये स्थितो धर्म

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

MIB'S ADVISORY ON DRUG DEPICTIONS IN OTT CONTENT

NEWS

The Ministry of Information and Broadcasting ('MIB') recently issued an advisory to OTT platforms concerning the depiction of narcotics and psychotropic substances. The advisory emphasizes that content should not glamorize or normalize drug use, particularly to protect younger audiences. It calls for stricter categorization of such material under the IT Rules, 2021, and mandates warnings about the harmful effects of drugs. It advises platforms to create public health messaging and cautioning against potential violations of the Narcotic Drugs and Psychotropic Substances Act, 1985 ('NDPS Act').

LEGAL TALK

The advisory reinforces the legal framework governing OTT content by urging platforms to exercise caution when portraying substance abuse. It categorizes sensitive content under higher classifications, issuing clear disclaimers, and adhering to public health messaging guidelines. However, terms like "glamorization" and "promotion" remain vague, leaving room for subjective interpretation. This uncertainty could lead platforms to adopt self-censorship, potentially limiting diverse narratives and creative storytelling. The advisory highlights a growing tension between creative freedom and regulatory oversight in the OTT space. Filmmakers and producers argue that such guidelines can interfere with the authenticity of narratives, especially when a subject like drug abuse is integral to the story. For example, films like Fashion or Udta Punjab realistically portrayed the consequences of substance abuse, but increased regulation might compromise such stories by prioritizing compliance over artistic integrity. OTT platforms, fearing potential penalties, may preemptively censor content, thereby restricting nuanced depictions of complex themes. Moreover, mandatory warnings and disclaimers, while crucial for public awareness, can disrupt the immersive experience of storytelling. Overemphasis on such elements could drive audiences towards pirated content, undermining both the creative and commercial objectives of the platforms.

THE WAY FORWARD

Striking a balance between responsible content regulation and creative freedom is important. The government needs to provide clearer definitions of what constitutes glamorizing or promoting drug use to avoid confusion and ensure fair enforcement. Instead of focusing solely on restrictions, encouraging the creation of educational and awareness-driven content about the dangers of substance abuse could be a more effective approach. The Ministry can address public health concerns by working closely with content creators, while still respecting the creative integrity of storytellers.

DOT NOTIFIES THE TELECOMMUNICATIONS (CRITICAL TELECOMMUNICATION INFRASTRUCTURE) RULES, 2024

NEWS

The Department of Telecommunications (DoT) has released the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024. These rules establish a framework to identify and protect critical components of India's telecommunication networks, aiming to enhance national security and ensure the resilience of essential communication services.

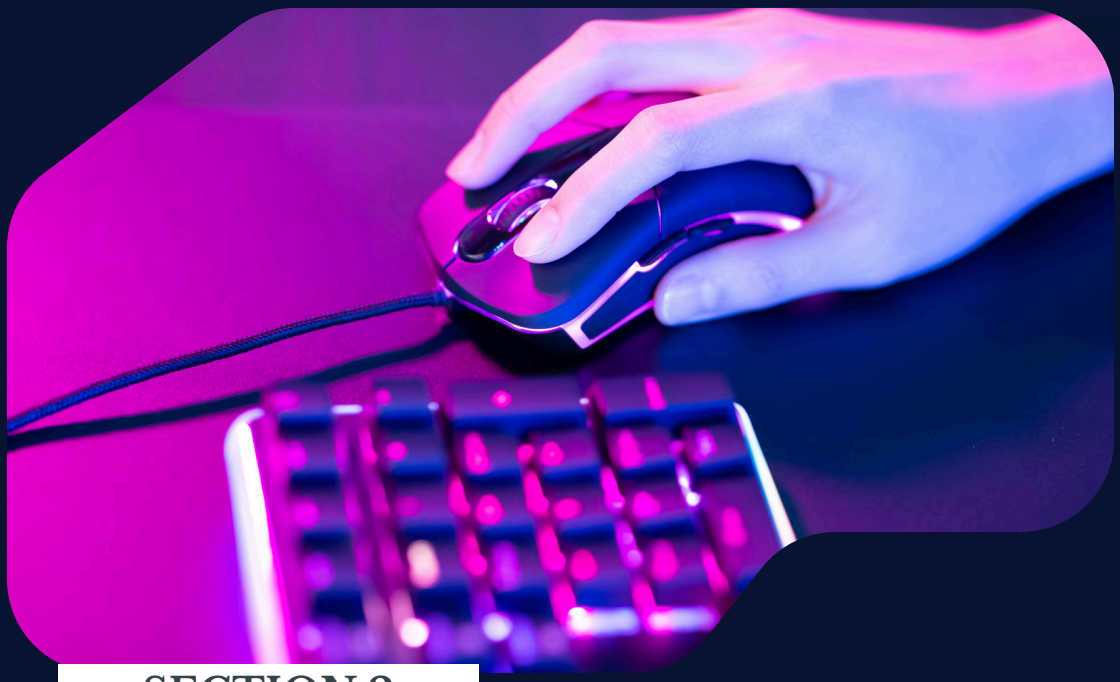
THE WAY FORWARD

The Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, present a robust regulatory framework. The Rules represent an opportunity to establish a precedent for secure and resilient telecommunications in a globally volatile digital environment. The emphasis on compliance and inspections underscores the move towards mitigating risks, and the success of the rules deepens on proper enforcement while also mitigating the many stakeholders' concerns. Clarity and elaboration in interpreting key provisions is also essential to ensure uniform and effective application. With transparent processes and oversight mechanisms, these Rules could effectively secure critical infrastructure without undermining innovation or market competition.

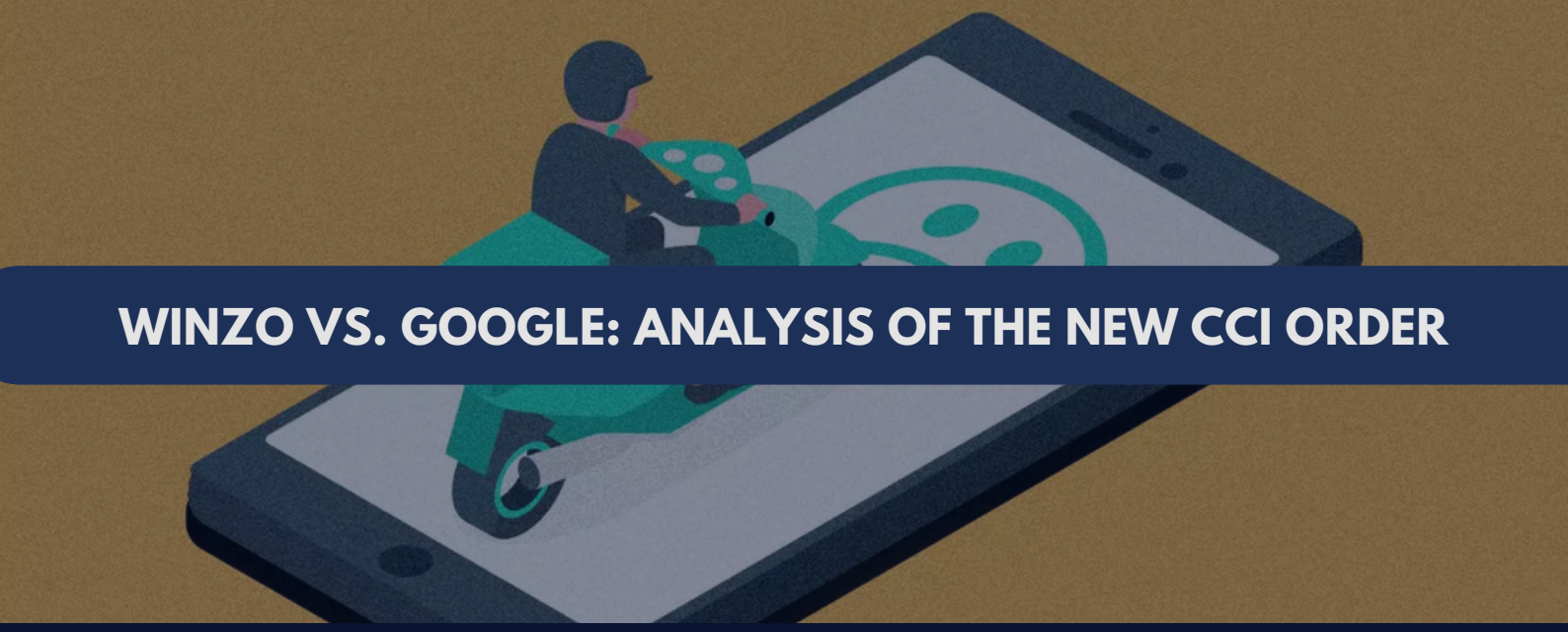
LEGAL TALK

The Rules define "Critical Telecommunication Infrastructure" ('CTI') as network components whose disruption could compromise national security, public safety, or economic stability and empower the Central Government to declare specific systems or networks as CTI. CTIs must adhere to comprehensive compliance measures, including aligning with Essential Requirements ('ER'), Interface Requirements ('IR'), and Indian Telecom Security Assurance Requirements ('ITSAR'). Operators are obligated to maintain detailed asset registers of their CTI, and report any security incidents within a six hour window. The rules also provide for the appointment of the Chief Telecommunication Security Officer ('CTSO') who will be responsible for implementing and overseeing compliance. The rules also establish protocols for routine inspections, vulnerability assessments, and enforcement mechanisms. The DoT retains authority to suspend operations or impose penalties for non-compliance. Additionally the Central Government is authorised to inspect the hardware, software and data of the CTI through the designated personnel. While these measures will undoubtedly strengthen cybersecurity, concerns arise about the proportionality of compliance costs and its impact on innovation and smaller players in the telecom industry. The Rules also mandate the preservation of logs and other data retention provisions. Numerous stakeholders have raised concerns about the government having excess powers to access and store the data. The rules also do not provide for safeguards like data minimisation, storage limitation etc. The Rules also provide for the identification of CTIs, however the assessment, based on 'impact on national security, economy, public health, or safety of the nation', has not been defined. The designation of CTI would subject telecom companies to stricter compliance and the lack of an exhaustive criteria can lead to potential arbitrariness.

Online Gaming and Betting Laws



SECTION 2



WINZO VS. GOOGLE: ANALYSIS OF THE NEW CCI ORDER

NEWS

WinZO Games has accused Google of restrictive practices, including the selective listing of Real Money Gaming ('RMG') apps like Daily Fantasy Sports ('DFS') and Rummy on its Play Store while excluding other skill-based games. Google's sideloading warnings, displayed when users attempt to download unlisted apps, have also been criticized for harming the reputation of developers like WinZO. Additionally, WinZO alleges that Google's advertising policies, which favour DFS and Rummy, restrict visibility and market access for other RMG developers.

LEGAL TALK

The legal proceedings have focused on multiple issues framed by the courts and the Competition Commission of India ('CCI'). The Delhi High Court analysed whether Google's warnings for sideloaded apps constitute disparagement, trademark infringement, or breach of contract. Observing that the warnings serve as general disclaimers consistent with industry standards and mandated by the IT Rules, 2021, the court ruled that these do not infringe on trademarks or tarnish WinZO's goodwill. The court further clarified that such warnings are intended to ensure user security rather than target specific developers. The CCI's examination delves into broader competition law concerns. It has preliminarily identified Google's dominance in markets for app stores, licensable operating systems, and online advertising. The selective inclusion of DFS and Rummy in Google's pilot program, coupled with extended grace periods, was flagged as potentially anti-competitive. The CCI highlighted how these actions could distort the RMG market by conferring undue advantages to specific apps, creating barriers for others, and denying equitable market access. Moreover, the CCI has raised concerns about Google's ad policy, which disproportionately limits promotional opportunities for non-DFS/ Rummy games. Additionally, it seeks to assess the justifications behind Google's selective approach to RMG apps, including whether such actions violate competition law by restricting the technical and scientific development of excluded apps.

THE WAY FORWARD

Resolving these disputes requires regulatory clarity and collaborative approaches. MEITY's proposed self-regulatory framework for RMGs could reduce ambiguity and ensure fair certification processes. Courts and regulatory bodies must also enforce a level playing field by addressing anti-competitive practices while balancing innovation with compliance. For its part, Google must re-evaluate its policies to avoid favouritism and ensure inclusive market access for all developers, fostering a healthier, more competitive ecosystem..

FinTech

SECTION 3

CENTRAL GOVERNMENT PROPOSES DRAFT LEGISLATION BANNING UNREGULATED DIGITAL LENDING ACTIVITIES

NEWS

The Central Government has proposed significant legislation to curb unregulated digital lending practices through the draft bill known as the Banning of Unregulated Lending Activities ('BULA'). The draft legislation is a designed move by the government to prohibit all lending activities that are not sanctioned by the Reserve Bank of India ('RBI') or other regulatory bodies. It aims at establishing a comprehensive framework for regulating digital and traditional lending practices.

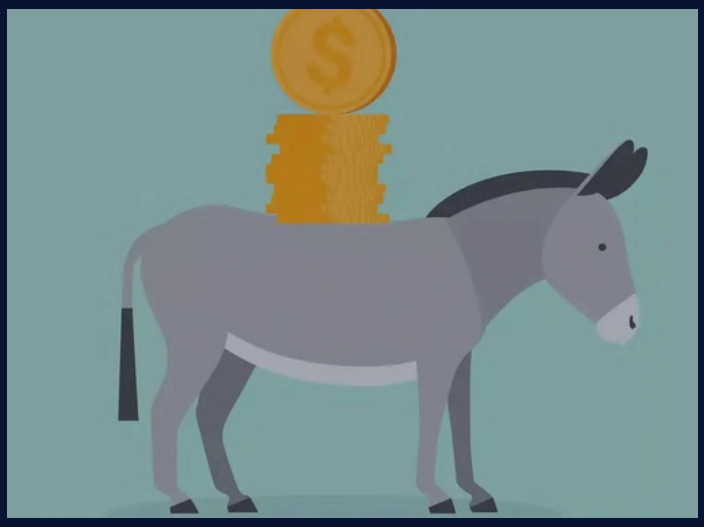
LEGAL TALK

Section 11 of the bill proposes that "any lender who offers loans, either digitally or otherwise, in violation of this law, shall be punishable with imprisonment for a minimum of two years, which may extend up to seven years, along with a fine ranging from Rs 2 lakh to Rs 1 crore. Lenders who use unlawful methods to harass borrowers or recover loans will face imprisonment from three to ten years and fines." A significant issue in the digital lending domain is the lack of transparency regarding the identity of the actual lenders, as consumers often have no physical interaction during the lending process. Therefore, prescribing stringent punishments will help in deterring the proliferation of unethical lending practices, especially in the growing digital lending sector. Further, under section 19, investigations should be transferred to the Central Bureau of Investigation ('CBI') if the lender, borrower, or properties are located in multiple states or union territories or if the total amount involved is of such magnitude to significantly affect public interest. This would ensure that cross-border investigations are conducted smoothly without jurisdictional conflicts. It also entrusts the process to an expert investigating agency for better efficiency and effectiveness. Other than this, under the First Schedule, 20 distinct laws governing regulated lending activities, such as the RBI Act, Banking Regulation Act, State Bank of India (SBI), Life Insurance Corporation (LIC), among others are listed to monitor digital lending. This would ensure that the lending activities in the market are in compliance with various laws and hence are periodically regulated. Additionally, under section 29, the Centre is empowered to amend the First Schedule in consultation with regulators which allows the government to exclude any regulated lending activity covered by the aforementioned legislations. Although, this may grant discretionary authority to the Centre to monitor the lending activities on a regular basis, yet the broad discretion is susceptible to challenges due to lack of specific criteria which raises concerns over arbitrary exclusions.

THE WAY FORWARD

Although the Bill manifests a proactive approach towards consumer protection in the world of digital lending, the legislation's success is dependent on its effective implementation and enforcement. The regulatory bodies are required to check for regulatory compliances and investigate any violations being made. Additionally, there is also a need to enhance public awareness through campaigns educating potential borrowers about their rights under this new legislation. Collectively, through the efforts of legislation, regulatory bodies and industry stakeholders consumers can be protected from digital fraud.

RBI INTRODUCES AI SOLUTION TO IDENTITY MULE BANK ACCOUNTS



NEWS

In a press release dated December 6, 2024, the Reserve Bank Innovation Hub ('**RBIH**') in Bengaluru announced the development of a pilot artificial intelligence ('**AI**') and machine learning ('**ML**') model called 'MuleHunter.AI.' Former Governor Shaktikanta Das emphasized that this system aims to significantly reduce instances of digital fraud in India's banking system.

LEGAL TALK

The RBIH has developed an in-house AI/ML-based model, MuleHunter.AI, to address the proliferation of mule accounts in the financial system. Leveraging advanced algorithms, the tool analyzes transactional and account-related datasets, enabling faster and more accurate detection of mule accounts compared to traditional rule-based systems.

- What is a Mule Account?

A mule account is a bank account used by criminals to launder illicit funds. These accounts are often created by unsuspecting individuals lured by promises of easy money or coerced into participation. The interconnected nature of such accounts complicates efforts to trace and recover funds. In India, mule accounts are often opened by Indian nationals offering their accounts for misuse in exchange for monetary benefits. This poses a significant challenge in detecting mule accounts during the account holder onboarding process.

- What are the current safeguards against it?

The Reserve Bank of India ('**RBI**') has tightened customer due diligence ('**CDD**') norms through amendments to its Master Direction on Know Your Customer ('**KYC**'). These updates align with government and Financial Action Task Force ('**FATF**') recommendations to combat money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

- Framework for AI in the Financial Sector

As a step in this direction, the RBI has proposed the establishment of a Framework for Responsible and Ethical Enablement of Artificial Intelligence ('FREE-AI') in the financial sector. To achieve this, a committee will be constituted comprising experts from diverse fields to recommend a robust, comprehensive, and adaptable AI framework for the financial sector. The details of the committee will be notified separately.

- Why was MuleHunter.ai developed?

Mule accounts play a central role in most online financial frauds in India. In the past year, the Centre froze approximately 4.5 lakh mule accounts linked to cybercrime proceeds. Banks are now urged to adopt advanced technologies like AI/ML and to foster inter-bank collaboration for improved detection and monitoring. While MuleHunter.AI is developed with the goal of detecting and preventing financial fraud, its development is tailored to the specific challenges and regulatory environment of India's banking sector.

By focusing on the identification of mule accounts, it addresses a critical issue in the country's financial ecosystem. The integration of such AI/ML-based solutions signifies a global shift towards more efficient and accurate financial crime detection mechanisms, moving beyond traditional rule-based systems to adaptive, intelligent technologies capable of responding to evolving fraudulent behaviors. Despite its innovative design, MuleHunter.AI faces several challenges common to AI-driven AML solutions. One major issue is data quality and availability, as inconsistent or incomplete data can lead to inaccuracies in detecting suspicious activities. Another challenge lies in integration with legacy systems, as many banks rely on outdated infrastructure that may not be compatible with advanced AI tools. Additionally, the explainability of AI models poses a hurdle; complex algorithms often function as "black boxes", AI systems whose inputs and operations aren't visible to the user, making it difficult to interpret their decisions and meet regulatory requirements. Ethical and privacy concerns also emerge due to the extensive data analysis required, raising questions about data security and public trust, therefore, adapting to evolving fraud techniques is critical, as fraudsters continuously develop new ways to bypass detection systems. To address these challenges, robust data governance frameworks and regular audits can ensure data quality and integrity. Developing flexible APIs and middleware solutions can facilitate smoother integration with legacy systems, supported by comprehensive IT training. Incorporating explainable AI (XAI) techniques can improve transparency and build trust among regulators and stakeholders. Adhering to strict data privacy laws, implementing strong security measures, and conducting ethical reviews can mitigate privacy concerns, continuous learning mechanisms and collaboration with other institutions to share insights on new fraud tactics can help MuleHunter.AI stay ahead of emerging threats.

THE WAY FORWARD

MuleHunter.AI, represents a significant advancement in detecting mule accounts within India's banking system. By leveraging advanced ML algorithms, it analyzes transaction patterns and account details to identify suspicious activities with greater accuracy and speed compared to traditional rule-based systems. In conclusion, while MuleHunter.AI represents a significant advancement in combating financial fraud within India's banking sector, addressing these potential challenges through proactive strategies will be essential to ensure its long-term effectiveness and reliability.

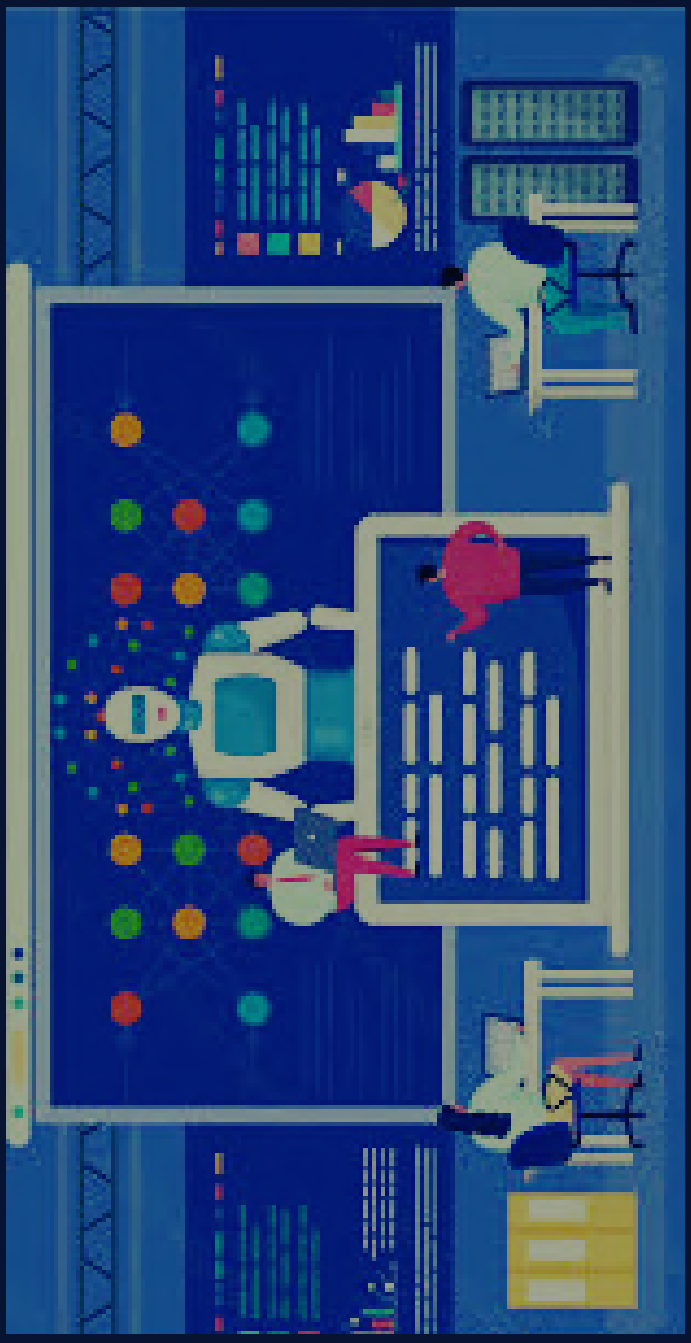
ARTIFICIAL INTELLIGENCE

SECTION 4

CONTINUING PERIL; OPENAI FACES COPYRIGHT CLAIMS IN CANADA

NEWS

OpenAI's troubles with news agencies don't appear to be at a close hiatus anytime soon. In a recent development, a massive claim has been pushed in Canada, at the Ontario Superior Court of Justice. This claim has been brought by established Canadian outlets, including The Globe and Mail, The Canadian Press, CBC, Toronto Star, Metroland Media, and Postmedia. This claim follows the patterns of a series of legal actions brought all over the globe over the year against OpenAI. In January of 2024, LexTech Newsletter covered the first of such claims by the New York Times concerning plagiarism by OpenAI. Even last month, we covered a similar litigation by Asian News International News Agency and the surprising outcome of another such claim in the USA. The News Agencies allege that AI companies are strip mining journalism by simply training their Large Language Models ('LLMs') over the resources generated by these bodies that are available on the Internet. They laid a massive claim of C$ 20,000 per article infringed, which could lead to billions of dollars in aggregate.



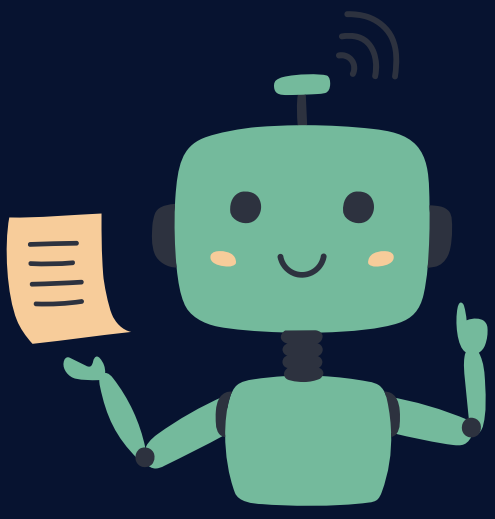
LEGAL TALK

While OpenAI is yet to file its response to these claims, a possible stance that is emerging out of statement released is that ANI takes great care in our products and design process to support news organisations, with emphasis on the fact that their usage of publicly available data adheres to 'Fair use' principles. While we shall analyse this speculated defence here, in the November edition of the Newsletter, we discussed certain other defences and actions being materialized by OpenAI. What is fair use is a question that varies from jurisdiction to jurisdiction. For example, in the USA, 'Fair use' is an affirmative right, not a justification for infringement. However in India, 'Fair use' was effectuated with the intention of securing the rights of authors in their own productions. This is probably why India lays out a whole range of specific acts that come in fair dealings, but the USA just provides a 'Four-factor Test' to determine 'Fair use'. News reporting for one, falls under the specified categories of fair dealings. But it remains to be analysed whether usage of 'Actual news reports' for claiming a defence under this head has any element of legality?

For this it becomes important to understand what constitutes “Fair” in the first place. In an important ratio of Kartar Singh Giani v Lodha Singh, it was found that unfairness is when there must be an intention to compete and to derive profit from such competition. If one puts OpenAI on this pedestal, their defence might fall flat on its face. This is because OpenAI has long lost its not-for-profit status and is now actively in business with multiple product ranges. In an American case of Swatch Grp. Mgmt. Servs. Ltd. v Bloomberg, the USA second circuit court observed that defence of reporting can be used when the purpose is actually to report these events and not anything else. If the work serves as a replacement in the market for sale of authorized copies of the original material, then this was found to be unjust.

THE WAY FORWARD

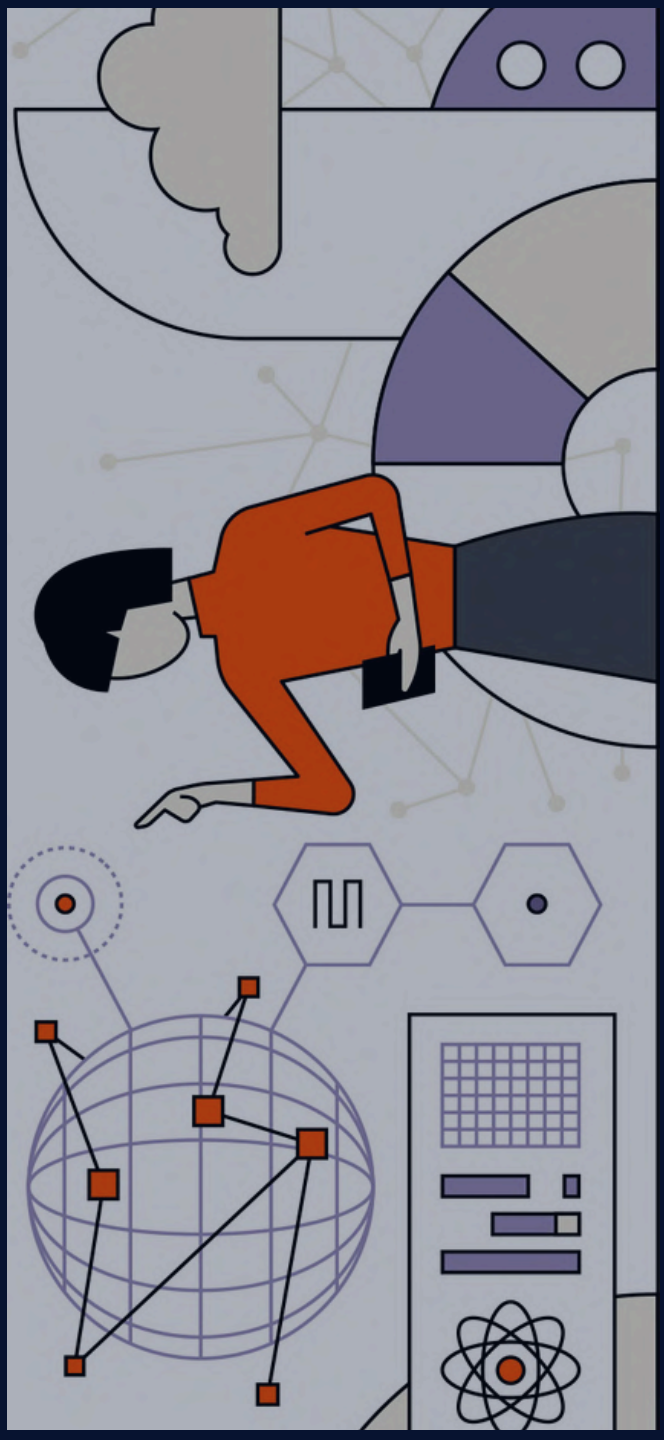
This understanding of the law of two jurisdictions is enough to understand the material weakness of such a defence. OpenAI is essentially packing the content of these websites and white labelling the same as their own. This is not even disputed because this is the way LLM engines work. The only legal way out possible for OpenAI is to deal with these claims outside the halls of justice and reroute its approach towards training its LLMs. Thankfully, and as we’ve covered in our previous editions, OpenAI is well set on its path to do the same and have already started incorporating material changes like ‘Opt-Out’ option and tying up with news agencies for data training.



NETHERLANDS EXPANDS INVESTMENT SCREENING LAWS TO INCLUDE ARTIFICIAL INTELLIGENCE AMONG THE OTHER EMERGING TECHNOLOGIES

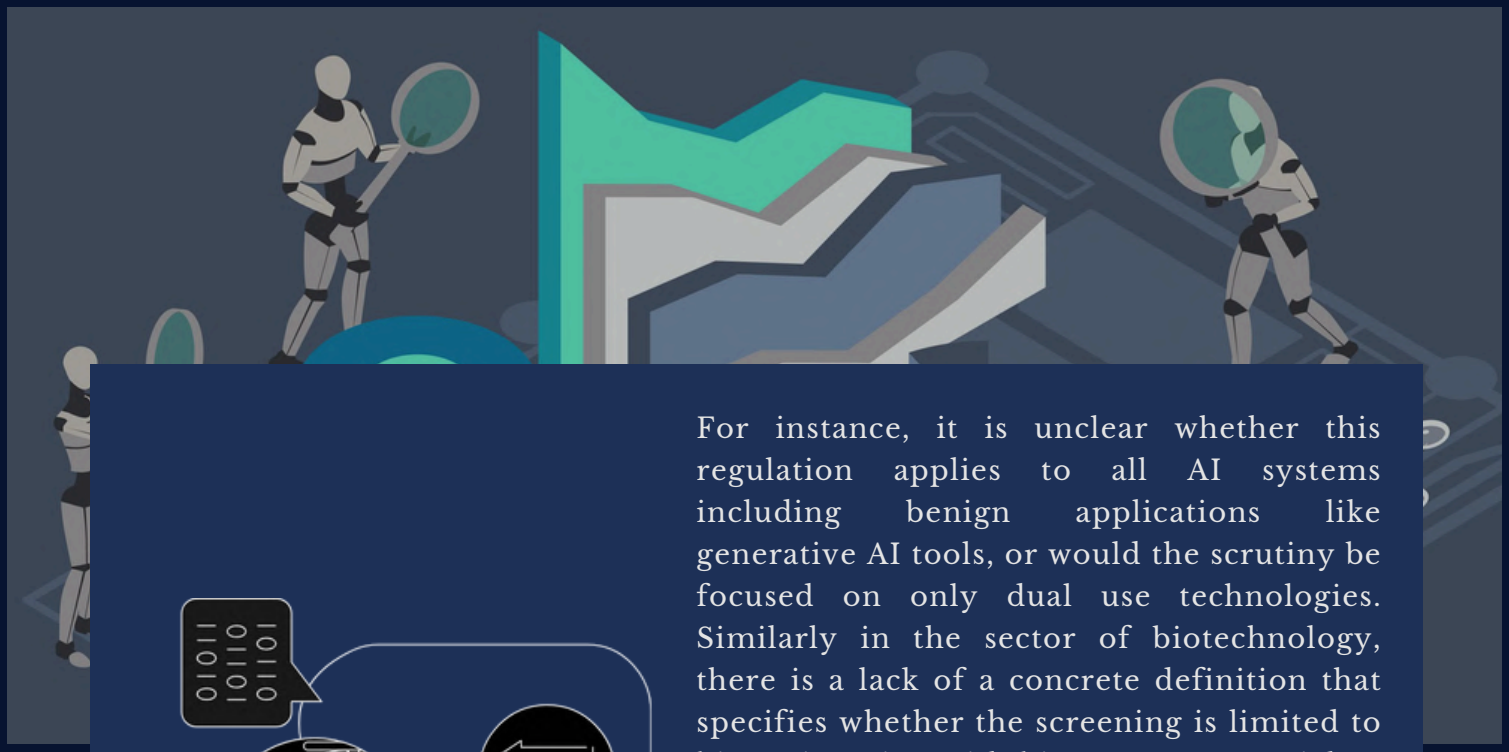
NEWS

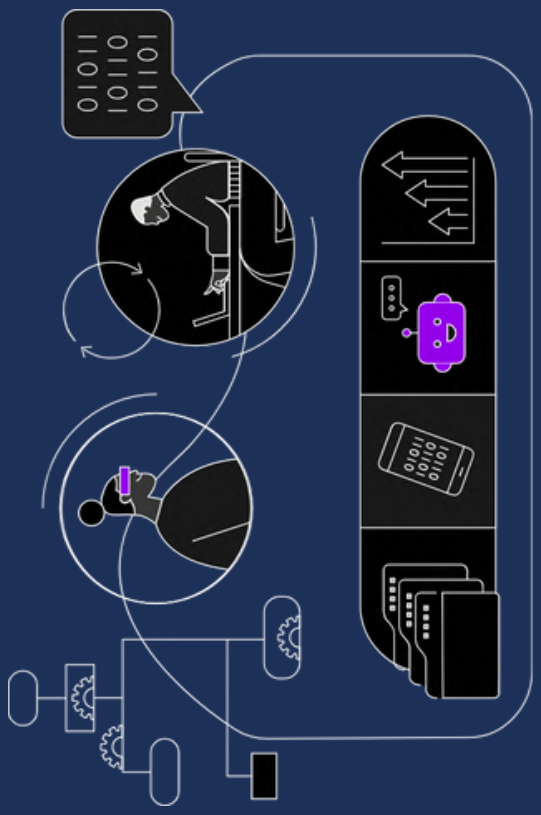
The Netherlands has recently released plans to expand the investment screening law to include AI, biotechnology, nanotechnology, sensor, and navigation technology among others. This decision comes in light of the emerging need to safeguard national security against threats like cyber operations, sabotage, and forms of espionage. The new rules are expected to come into force during the second half of 2025 and currently, the domestic laws mandate notifications for investments affecting critical infrastructure or technology. By broadening the scope of sectors subject to investment scrutiny, the Netherlands aims to mitigate risks in strategically significant sectors and industries and reflects growing concerns about the potential misuse of emerging technologies.



LEGAL TALK

The Dutch government's proposal to expand the VIFO Act (*Wet veiligheidstoets investeringen, fusies en overnames*) builds on its framework for regulating investments in critical infrastructure and sensitive technologies to protect national security. Currently, sensitive technologies as defined under the VIFO Act, includes significant sectors with dual-use potential; such as those concerning cyber security, defense sectors, and critical data infrastructures. The proposed amendment is now going to incorporate the emerging sectors such as biotechnology, artificial intelligence, medical nuclear technologies among the notable areas. The inclusion of sectors such as AI and other emerging technologies under this law is in line with the obligations the Netherlands is required to observe under EU Regulation 2019/452. Under this regulation, member states are mandated to adopt mechanisms that address public order and security risks arising from foreign direct investments in sensitive sectors. Hence, the legal basis for the expansion of this law is sound and in line with the EU directives. However, there remains an ambiguity in regards to the scope of this regulation.





For instance, it is unclear whether this regulation applies to all AI systems including benign applications like generative AI tools, or would the scrutiny be focused on only dual use technologies. Similarly in the sector of biotechnology, there is a lack of a concrete definition that specifies whether the screening is limited to bioengineering with bioweapon potential or it may extend to the pharmaceutical industry, unrelated to the security concerns. The current definitions of "sensitive technologies" may be perceived as excessively broad alongside the lack of clearcut thresholds for triggering regulatory review which could lead to overregulation. The refinement of the legal framework is also warranted in consideration of the dual-use challenges that technologies under AI and Biotechnology present. The application of the same extends from healthcare to matters of national defense which must be recognized by the law to be able to sophisticatedly differentiate between benign and high risk investments and ensure that there is no hindrance to legitimate trade deals.

THE WAY FORWARD

The Netherlands must approach a balanced and transparent approach to the expansion of the investment laws to approach the dual objectives of maintaining national security while still retaining the interest of foreign investors in the country. Collaborating with industry leaders and EU partners in the interest of harmonizing standards and avoiding market fragmentation is a crucial step. Introducing clear and precise definitions; especially specifying the ambit of "sensitive technologies" would ensure regulatory clarity and minimize ambiguity. Additionally, the government may establish criterias for identifying high-risk investments, outline notifications, guidelines, and review procedures to minimise uncertainty for investors. To reduce the escalation of disputes to the scale of WTO and other international bodies, the government may consider setting a domestic recourse for investors who seek to challenge decisions that may be perceived as arbitrary or excessive.

DATA PRIVACY

SECTION 5

SEBI'S NEW DATA SHARING POLICY: BALANCING MARKET TRANSPARENCY AND PRIVACY

NEWS

The Securities Exchange Board of India ('SEBI') has proposed a transformative draft policy, "Policy for Sharing Data for Research/Analysis," ('Draft Policy') aiming to revamp data access in India's financial markets. This initiative updates SEBI's 2018 policy, addressing its limitations and aligning with the Digital Personal Data Protection Act ('DPDPA'), 2023.

LEGAL TALK

The draft policy is a milestone for data governance in Indian financial markets. It reflects SEBI's commitment to balancing data democratization with privacy safeguards. It incorporates principles of data minimization and purpose limitation, aligning with DPDPA's dual objectives. While expanding data access for researchers, the policy mandates strict protocols to prevent misuse, including SEBI's audit rights. The draft introduces a two-basket approach, categorising data into shareable data like anonymized market statistics and non-shareable data such as personal PAN details. The policy empowers Market Infrastructure Institutions ('MIIs') to establish their data-sharing guidelines, reducing SEBI's operational load while enhancing data availability. The policy also promotes ethical data handling, ensuring compliance with data privacy and governance norms. Additionally, MIIs are tasked with developing compliant frameworks, making them important in the new ecosystem. However, challenges like infrastructure readiness and consistent implementation highlight the need for phased rollouts and standardized oversight mechanisms.

THE WAY FORWARD

For successful implementation, SEBI must provide phased guidelines and robust support to MIIs to adapt to the new norms. Regular compliance training can bridge the gap between policy and practice. Standardized oversight, coupled with periodic audits, can address concerns about data misuse. By setting a high standard for data sharing and governance, this policy could serve as a model for other sectors, fostering innovation while safeguarding privacy.

EDPB'S OPINION ON PROCESSING OF PERSONAL DATA BY AI MODELS

NEWS

On 17 December 2024, the European Data Protection Board ('EDPB') issued an opinion under Article 64 of the General Data Protection Regulation ('GDPR') on the data protection aspects related to the processing of personal data in the context of AI models. This was done on request of the supervisory authority in Ireland.

LEGAL TALK

The EDPB issues legal opinions on various matters when requested by supervisory authorities intending to adopt specific decisions. These opinions guide GDPR application across Member States on matters of general impact or cross-border significance. While not legally binding, they strongly influence investigations and enforcement procedures. The current opinion is globally unique, providing critical insights into applying GDPR principles to AI models. The Irish authorities posed key questions about processing personal data in AI models, such as whether AI models meet GDPR's definition of personal data, how legitimate interests can justify processing, and the impact of unlawfully processed data on AI model operations. They also inquired about balancing data controllers' interests with those of data subjects and ensuring no personal data is processed. The EDPB clarified that AI models trained on personal data cannot always be considered anonymous. Even when not explicitly designed to identify individuals, models may absorb information in their parameters, making it extractable. Supervisory authorities ('SAs') must assess claims of anonymity case-by-case, considering whether personal data can be extracted or inferred and ensuring measures prevent unintended reuse or disclosure. The EDPB addressed legitimate interest as a lawful basis for processing under GDPR Article 6(1)(f). Controllers must meet three conditions: demonstrate a legitimate interest, show the processing is necessary, and ensure it does not override data subjects' rights.

SAs must scrutinize whether personal data use is indispensable, particularly during AI development, and ensure compliance with the data minimization principle. The EDPB also emphasizes maintaining comprehensive documentation to prove the design and functioning of AI models. The opinion permits controllers to rely on legitimate interests for developing and deploying AI models, including training on public data, but demands case-by-case assessments. It imposes stringent standards for necessity, likely complicating large language model ('LLM') development. The EDPB also recognizes that anonymized AI models exempt companies from privacy obligations related to personal data. In such cases, developers need only ensure data misuse is prevented. While the opinion holds greater relevance in the EU, where even public data requires consent for training, it highlights practical approaches applicable elsewhere. For example, developers can seek consent by assuring individuals that outputs remain anonymized. However, the opinion leaves several AI-related issues unaddressed and uses ambiguous language, complicating its practical application.

THE WAY FORWARD

This opinion tackles critical grey areas in data processing for large language models, adopting a progressive yet challenging approach. While the global trend leans toward outright bans on using personal data in AI training, the EDPB recognizes the necessity of these datasets and seeks to establish a middle ground. It offers exemptions for companies to enable innovation while safeguarding data privacy. However, despite being a positive step, the EDPB has set exceptionally high compliance standards, making it difficult for companies to meet these requirements in practice. This may hinder development efforts and create significant operational challenges for AI innovators.

INDIA'S SAFEGUARDS TO THE CAMBRIDGE ANALYTICA SCANDAL

NEWS

The Australian Information Commissioner finally settled its long-pending case against Meta Platforms over the Cambridge Analytica Scandal. According to the lawsuit, Meta shared personal user data with the "This is Your Digital Life" personality quiz app. The data was eventually used to create voter profiles and target political ads.

LEGAL TALK

Data minimization is the one principle that can safeguard the kind of data that social media giants procure from users but the problem with this is that unlike the GDPR which points out the principle and draws the line of accountability, the DPDP Act merely mentions it in the context of processing personal data based on consent and puts the entire burden of understanding how the data can be used by the data fiduciary on the data principal. The core issue of the scandal was that the Facebook users unknowingly allowed their data to be harvested by a third-party quiz app, which was then shared with the Cambridge Analytica firm. In India, although section 6 of DPDP Act specifies that the consent obtained must be free, specific, informed etc., there also exists certain broad exemptions under Section 17 of the Act which provide loopholes for third-party entities to get access to users' personal data without their consent on the pretext of collecting it for the purpose of national interest or to maintain public order. There are high chances that such data can be used for political campaigns or other purposes and thereby get misused. Thus, the Act should clearly define "national interest" and "public order" and ensure oversight from the Data Protection Board to verify that the data collected is being used for legitimate purposes only.

THE WAY FORWARD

Facebook uses automated-decision making to target users with specific content and shows ads and posts relating to that thereby trying to influence their opinions. To combat this, India could bring in a regulation wherein the users would be allowed to regulate the kind of content that they want on their social media accounts. Currently, Facebook only allows the users to stop ads based on certain categories but it is imperative that the users be allowed to control the content as well as ads they see to avoid being manipulated. Additionally, the penalties imposed under the Act are satisfactory, they are not stringent enough for large-scale violations, and therefore the fine should be proportional to the harm caused and the revenue generated from the misuse. The DPDP Act will prove to be effective but its effectiveness will be truly fruitful only when it portrays the ability to evolve alongside the dynamic digital landscape.

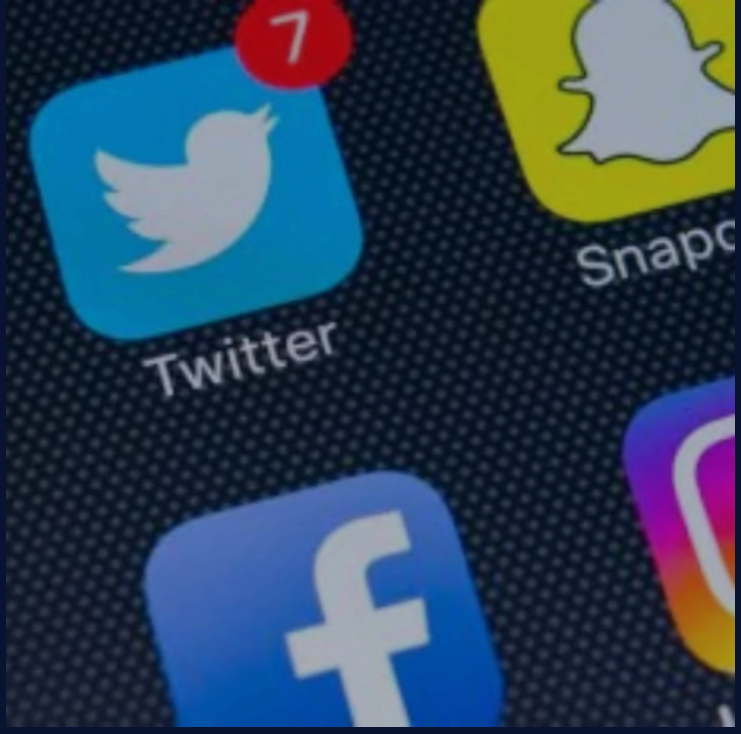
AUSTRALIA'S SOCIAL MEDIA BAN

NEWS

Australia has implemented one of the world's strictest internet crackdowns, banning children under 16 from using social media or creating new accounts. Authorities have not finalized the list of restricted platforms, but it is expected to include apps like Snapchat, TikTok, Instagram, and X.

LEGAL TALK

The government introduces amendments to the existing framework, which will take effect a year from now. It holds social media companies responsible for verifying the ages of children, with more detailed guidelines to follow soon. Failure to comply could result in fines of up to nearly $50 million. Social media platforms themselves will be responsible for implementing these verification processes, and they will not be permitted to collect user information to prove that reasonable efforts are being made from their side to adhere to the law, unless no other alternatives exist. Even then, any such data must be destroyed once the user's age is verified. The government has carefully crafted its approach to reduce privacy risks. Companies cannot rely solely on government IDs for age verification; they must use alternative methods, allowing users to avoid sharing sensitive personal information tied to their ID. Likely alternatives include AI tools for biometrics and other verification technologies —- and privacy concerns related to these are minimised by the mandate in Section 63F(3) to destroy user data. However, a potential loophole remains: while the mandate applies to social media platforms, it does not extend to the AI tools themselves. This means AI tools could still collect data, opening the door to widespread tracking and misuse. At the same time, there are other concerns regarding unreasonable restrictions on free speech. Alternative methods to government ID verification could raise compliance costs.



Systems like biometrics could be easily bypassed by users, for example, through Virtual Private Networks (VPNs), which weakens the security of the verification process. In this scenario, platforms would unfairly bear the responsibility of ensuring compliance. The accuracy of such verification mechanisms is also questionable. The definition of age-restricted social media platforms under Section 63C is broad and vague, meaning many online services could fall under its scope. While the law explicitly exempts messaging apps and gaming apps, it becomes unclear where platforms that serve as both social media and messaging services would fall, creating a grey area.

When analyzing the effectiveness of any law, it is important to assess its intent and whether it achieves its goals. The Prime Minister has stated that the law aims to prevent the "harm" caused to children by the known negative effects of social media. However, this raises the question of whether this approach is truly the best one. Blocking children from social media entirely might drive them to darker, less regulated areas of the internet where no community guidelines, safety tools, or protections exist. While the intention to protect children is commendable, it could be achieved through alternative means that have fewer side effects. One such option is to simply regulate the content accessed by younger users. Platforms could be held accountable for disseminating harmful or dangerous content, encouraging them to monitor the content more closely. Legal standards could be established that place a duty of care on platforms to ensure their products are safe for children. Additionally, introducing parental consent exemptions, as seen in France, could be a practical solution. It is not the government's role to act as a parent if the child's parents approve the usage. Although enforcement challenges may arise with such parental consent mechanisms, this approach is better suited to balance privacy concerns with fundamental rights. Similarly, the government could engage with social media platforms to explore ways of limiting the functionality of certain apps, rather than blocking them entirely. By reducing their features, the government could ensure that harmful, addictive, or dark design patterns are mitigated. Platforms could be encouraged to create "safe mode" options for younger users, offering curated content that avoids profiling, restricts interactions, and provides access to mental health resources. This approach would allow the government to address the issues without resorting to an all-or-nothing solution.

THE WAY FORWARD

Social media offers significant benefits, despite its challenges. For many teenagers, the anonymity of these platforms serves as a powerful outlet for self-expression and fosters a sense of community, especially for vulnerable groups like those facing bullying or from the LGBTQ+ community. It also enables global connections and provides a comfortable source of income, even for children. While defining 'dangerous content' is clear, terms like 'hateful' remain vague, complicating enforcement. Access to diverse opinions is crucial for independent thought in the future generation, a cornerstone of democracy. Rather than restricting access, solutions should focus on regulating content. Tools like education, such as Finland's digital citizenship curriculum, can help children navigate online spaces safely and develop digital resilience. Thoughtful regulation, though complex, is more effective than quick fixes like bans, which rarely resolve deeper issues. A similar law in Utah was deemed unconstitutional, highlighting the delicate balance between regulation and rights. This further underscores the need for carefully crafted approaches. The success of such laws will depend on their implementation, and if effective, could inspire global legislation (ironically this is the primary concern for social media platforms).

CONTRIBUTORS

WRITERS

ANJALI PANDE

TRISHNA AGRAWALLA

PRATYUSH SINGH

ANANYA SONAKIYA

MAITHILI DUBEY

BHAVYA BHASKAR

ALOK SINGH MOURYA

SATVIK MITTAL

EDITORS

HARSH MITTAL

LAVANYA CHETWANI

DESIGNERS

TRISHNA AGRAWALLA

ARUNIMA RAMAN

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL