LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

OCTOBER 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

यतो धर्मस्ततो जयः

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

MEITY ISSUES STRICTER COMPLIANCE DEMANDS TO INTERMEDIARIES

NEWS

Intermediaries in India are now under increased pressure to meet stringent due diligence obligations for content moderation and grievance redressal, as directed by the new advisory released by the Ministry of Electronics and Information Technology (‘**MeITY**’) on 3rd September 2024. This strict directive comes in light of the Bombay High Court order in the *National Stock Exchange v. Meta*, which flagged a genuine concern that failure to act promptly on harmful content may result in the loss of legal immunity and heightened liability risks. The necessity for intermediaries to adhere to their due diligence obligations under the IT Rules 2021, is reiterated through their advisory, targeting the rapid removal of harmful and misleading content to mitigate risks to public trust and safety.

LEGAL TALK

The MeITY advisory underscores the regulatory pressures on intermediaries to meet stringent compliance timelines or risk losing the safe harbour protection under Section 79 of the IT Act. For instance, after receiving a notice under Rule 3 of the IT Rules, intermediaries must delete unlawful content within 36 hours. While imposition of such rigid deadlines is done with the intention of maintaining safe harbor protection, it does raise questions about the operational feasibility among many other questions such as the risk of over-censorship.The interim responses related to user grievances are required to be addressed within specified timeframes. In addition, significant social media intermediaries are required to submit periodic monthly compliance reports and maintain 24/7 contact with law enforcement. However there is an absence of any mention of review mechanisms in cases of ambiguous/borderline content and clear procedural safeguards which may raise concerns and should be actively looked into. The intermediaries are additionally expected to proactively enhance their compliance frameworks. The advisory suggests establishing internal controls, regular audits, and coordination with government agencies to address harmful content. The case of NSE v. Meta highlights judicial intolerance for delays in removing content that could harm public or investor confidence, as the court ordered Meta to delete misleading videos within ten hours. The advisory further hints towards stricter monitoring with the hope that this trend would move towards higher degrees of monitoring, nudging these platforms to delete flagged content quickly to mitigate the risk of reputational or financial harm.

Although these principles propel timely content regulation, there have been fears that content may potentially be over-censored because of this systematised automatic process of content moderation. The balance between proactive compliance and that which will protect free expression is extremely delicate, especially for nuanced or ambiguous content. The tools utilised for content moderation would most probably be reliant on AI and algorithm which does work well for clear cut cases of explicit content but may pose an issue in deciphering nuanced issues like criticism, satire or political commentary. The focus on the timeline may force such content out of picture, potentially stifling legitmitate discourse on public issues or political matters. To mitigate this risk, companies can make periodic transparency reports to help users understand the basis of their platform's content removal and to show regulators that the platform is making measured decisions. The advisory's encouragement for periodic audits may provide an opportunity for platforms to continuously refine and adapt their moderation practices, minimising over-censorhip.

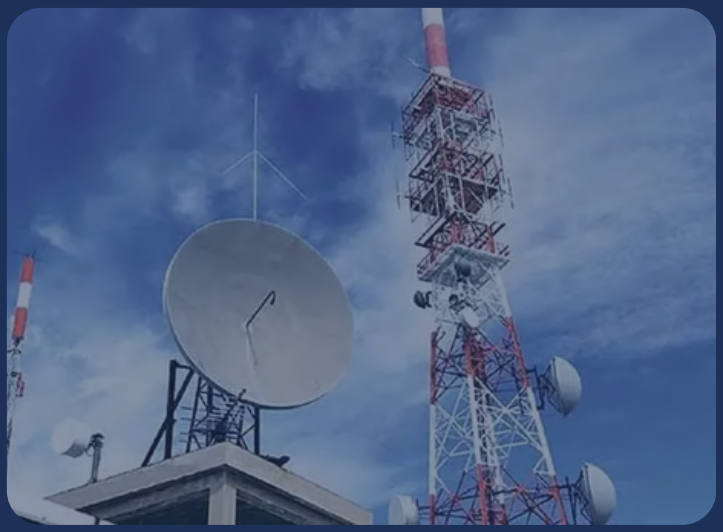
THE WAY FORWARD

To meet the strict compliance expectations, intermediaries may have to invest in sophisticated monitoring technologies, rigorous audits, and periodic training in content moderation teams. In the spirit of achieving accountability while protecting the digital ecosystem from misuse, the advisory for intermediaries on MeITY encourages intermediate parties toward compliance via the review of various and extensive stakeholder engagement that collectively leads to a safe and responsible online environment. An initiative may also be considered in setting up independent advisory boards with representation from legal, ethical and technological experts; this may help intermediaries balance the demands of regulatory compliance while still upholding user rights. Such efforts safeguard public safety without losing the necessary freedoms in digital expression by emphasizing timely and accountable content management.

TRAI ISSUES RECOMMENDATIONS FOR A SIMPLIFIED SERVICE AUTHORISATION FRAMEWORK UNDER TELECOMMUNICATIONS ACT, 2023

NEWS

The Telecom Regulatory Authority of India ('**TRAI**') has released recommendations for a new authorisation framework under the Telecommunications Act, 2023, proposing a shift from traditional licensing to a streamlined authorisation model.



THE WAY FORWARD

TRAI's recommendations advocate for a balanced approach that supports innovation without over-regulation. However, certain recommendations, like cloud integration, may require careful regulatory oversight to address data privacy and cybersecurity issues. Engaging stakeholders would ensure that cloud-based telecom services adhere to both telecom and data protection regulations. Looking forward, TRAI's proposal could significantly enhance India's telecommunications landscape by reducing barriers for smaller players and increasing flexibility for established providers. However, industry experts have cautioned that implementing a simplified regime without compromising regulatory checks will be essential to avoid market abuses and ensure consumer protection.

LEGAL TALK

TRAI's recommendations signify a move toward a more flexible, authorisation-based framework, replacing traditional licences. A key recommendation is the introduction of a Unified Service Authorisation ('**USA**'), allowing telecom providers to offer multiple services under a single authorisation. New authorisations would integrate services like cloud-based private phone systems (EPABX) under telecom authorisations. It aims to make it easier for providers to deliver multiple telecom services, thereby simplifying compliance. With the USA, providers can offer multiple services [voice, internet, and machine-to-machine ('**M2M**') communication] under one umbrella, potentially reducing redundant approvals and operational overheads. This change aligns with international models where telecom operators often have one primary authorisation, allowing broader service flexibility. Notably, TRAI proposed classifying authorisations into three categories: Main, Auxiliary, and Captive Service Authorisations. Main authorisations would cover primary services like access and internet services, while Auxiliary and Captive authorisations address specific needs, such as M2M connectivity and private network setups. Furthermore, the inclusion of cloud-based services under telecom authorisations reflects TRAI's attempt to bridge traditional telecom and digital service providers, addressing industry calls for enhanced regulatory clarity and encouraging cloud adoption within the telecom sector. The recommendations also propose a simplified financial regime with reduced entry fees and eased bank guarantee requirements, aiming to enhance market competition and lower compliance burdens for providers. The framework also introduces measures for enhanced infrastructure sharing, especially for 5G, which could reduce capital costs and increase regulatory efficiency in India's telecommunications sector.

MEITY'S NEW ADVISORY: TACKLING THE RISING THREAT OF BOMB HOAXES

NEWS

In response to a recent wave of hoax bomb threats affecting the aviation sector, the Ministry of Electronics and Information Technology ('**MeITY**') has issued an advisory dated 25th October 2024 underlining the timely completion of due diligence requirements under the Information Technology Act ('**IT Act**') and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('**IT Rules**').

LEGAL TALK

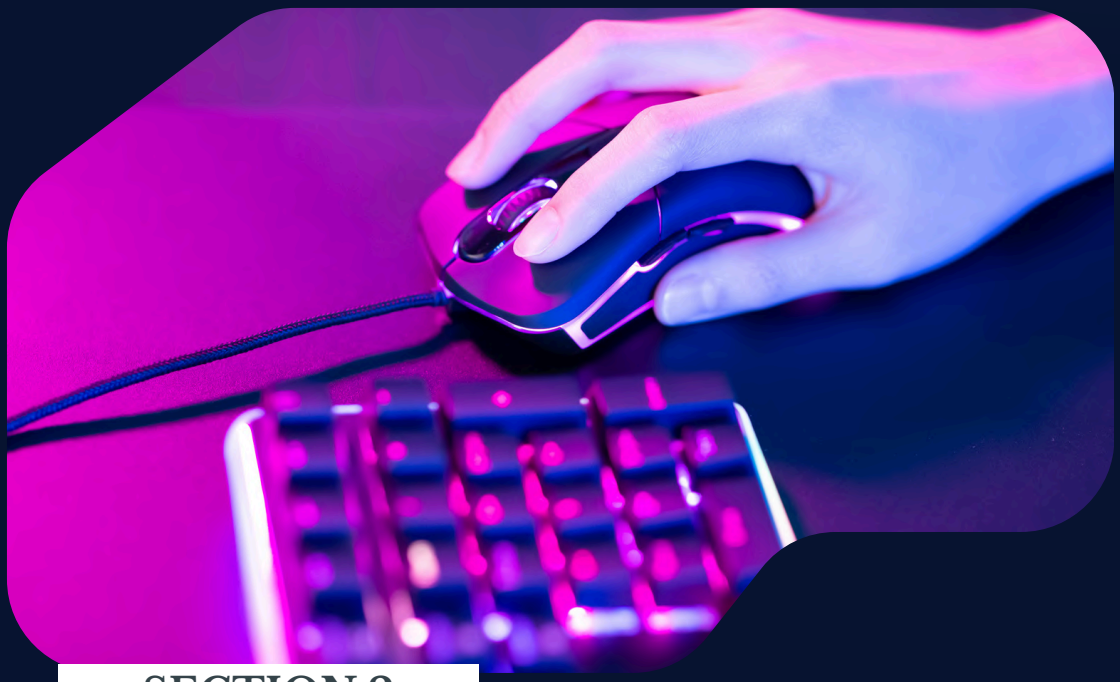
The advisory notes that features like forwarding and re-sharing have contributed to the "dangerously unrestrained" dissemination of fake threats, endangering public order, state security, and the operational security of airlines. MeITY directed social media intermediaries, to prevent users from hosting or sharing false or unlawful information, invoking language similar to Section 69A of the IT Act to emphasise the impact of hoaxes and that such 'misinformation' should be promptly removed. The advisory further instructed intermediaries to report such threats to authorities within 72 hours and reminded them that failing to follow due diligence requirements could nullify their safe harbour immunity under Section 79 of the IT Act. The advisory aligns with the new BNSS framework, which mandates intermediaries to report certain offences perceived to threaten national unity, security, or economic interests. Although the advis-

-ory is well-intentioned, it raises several concerns. Rule 3(1)(b)(v) of the IT Rules requires platforms to prevent the intentional sharing of "patently false" information, though terms like "false" and "untrue" lack clear definitions. Such ambiguities make it challenging for platforms to assess content accurately, potentially restricting free speech beyond Article 19(2) of the Constitution. While the advisory suggests treating such threats as "unlawful information" under Rule 3(1)(d) of the IT Rules, this raises practical concerns, as it requires the intermediaries to have "actual knowledge" of any violation via a court order or government notification before action is taken. Moreover, under Section 33 of the BNSS, every person "aware" of the commission of any offence under the BNS is obliged to report it. However, given the fact platforms do not have "actual knowledge" in this case, it is unclear how the BNSS' reporting obligation interplays with the IT Act and IT Rules.

THE WAY FORWARD

While holding social media platforms accountable for harmful content is a valuable objective, MeitY's advisory raises questions about the practical execution of these responsibilities. The current direction may impose undue burdens on intermediaries by requiring them to interpret ambiguous terms and take on roles that lack clear legal frameworks, potentially stifling free expression. Ensuring robust content monitoring and clear protocols can help intermediaries align with regulatory expectations. However, for effective enforcement, additional clarifications and refinements in the advisory are necessary to provide clear, balanced, and enforceable obligations.

Online Gaming and Betting Laws



SECTION 2

UK GOVERNMENT TO HIKE GAMBLING TAX RATES AMIDST INDUSTRY CONCERNS

NEWS

In a move that has stirred debate across the board, the incumbent Labour Party government has proposed a tax hike on the gambling industry, aiming to address rising concerns over gambling addiction and to generate additional revenue for public services. The tax increase would primarily affect online betting, casinos, and other gambling platforms. Party leaders argue that this measure is necessary to curb problem gambling, particularly among vulnerable populations, and to modernise the industry's regulatory framework. This proposal comes amid ongoing discussions around the review of the Gambling Act 2005, with calls for stricter regulations on advertising and player protections.

LEGAL TALK

Currently, the primary legislation that governs this industry is the 2005 Act, which regulates all forms of gambling including online betting. This law was designed to provide a flexible regulatory structure while promoting fair practices, protecting children and vulnerable individuals, and preventing gambling from being a source of crime or disorder. However, the Labour Party has criticised the act for not keeping pace with the growth of online gambling, leaving gaps in player protection and addiction support services. The proposed tax hikes would primarily target operators of online sports betting and casino games. Online operators are subject to a 21% Remote Gaming Duty ('RGD') under the Finance Act 2014, which governs taxation on remote gaming activities like online casinos. Labour's plan aims to increase this rate, with the exact figure yet to be disclosed. The party's stance is that online gambling companies, particularly those based offshore but operating in the UK, are reaping significant profits while not contributing enough to mitigate the social harm caused by their services. The proposed tax hikes could lead to increased scrutiny and tighter restrictions on overseas operators, closing loopholes that allow companies to benefit from lower taxes in jurisdictions like Gibraltar or Malta while targeting UK users. The amendments would require offshore operators to contribute more substantially to the UK economy through higher taxes or potentially risk losing their licences. The Labour Party has also emphasised the need for stronger provisions on player self-exclusion and time limits on online betting, to ensure consumers are better protected from the risks of compulsive gambling.

THE WAY FORWARD

The debate surrounding Labour's proposed tax hikes is likely to intensify, with questions over how to balance economic interests with consumer protection. With a general section of the public in support of the proposed amendment, a careful approach is needed to prevent unintended consequences, such as driving gamblers to unregulated platforms at the same time while balancing the concerns of industry members.

FRANCE CONSIDERS LEGALIZING ONLINE CASINOS IN 2025

NEWS

France could see regulated online casino as early as next year after the government sought to legalise the activity in its budget. The government added an amendment to the Draft Finance Bill 2025 which would introduce a licensed online casino market. It comes as prime minister Michel Barnier aims to slash the country's budget deficit to below 5% of GDP, down from its current level of 6.1%.

LEGAL TALK

France's move to regulate online casinos represents a strategic shift in digital gambling governance. The proposed dual layer taxation structure (27% Gross Gaming Revenue+social security levies totaling 55.6%) creates a robust fiscal framework while potentially serving as a compliance enforcement mechanism. This move aligns with the EU's broader trend toward regulated online gambling markets, but France's tax rate would be notably higher than other jurisdictions. The high taxation could serve two purposes: generating substantial state revenue and creating a barrier to entry that ensures only well-established, compliant operators enter the market. However,the success of this framework will likely depend on whether the tax burden allows operators to offer competitive enough odds to effectively combat the black market. Implementation would require sophisticated technical infrastructure for real time revenue tracking, anti money laundering compliance and cross border transaction monitoring.

THE WAY FORWARD

This regulation will potentially impact the revenue and jobs of land based casinos.This will also affect the local crime rates and a likely change to social dynamics.An enhanced security measure is required to counter this issue.The decision to legalise online casino games will likely continue to stir debate in the coming months as the country balances fiscal recovery with concerns about public health and industry stability.

FinTech

SECTION 3

GOVT AND FINTECHS COLLABORATE ON INDIGENOUS AML SYSTEM TO STRENGTHEN INDIA'S FINANCIAL SECURITY

NEWS

The government is collaborating with fintech companies to develop a new anti-money laundering ('**AML**') system targeting local financial frauds. This initiative involves geotagging transactions, forming a suspicious registry, and quicker fraud recovery, complementing existing mechanisms like Citizen Financial Cyber Frauds Reporting and Management System ('**CFCFRMS**') and involving new regulatory and cybersecurity measures.

LEGAL TALK

The initiative seeks to address issues such as mule accounts (*bank accounts that facilitate illegal transactions*), ensure faster recovery of defrauded money, and introduce geotagging for digital transactions (*the process of capturing the geographical coordinates of payment touch points used by merchants to collect payments from customers*). The geotagging of transactions raises concerns about data privacy and surveillance, especially with the Personal Data Protection Bill still under deliberation, ensuring that the new system adheres to global standards such as the EU's GDPR or FATF's AML recommendations would be crucial in maintaining user trust and international credibility. A key feature in achieving this is the creation of a "*suspicious registry*" for banking correspondents involved in fraud. This system will complement the existing CFCFRMS and involve new regulatory and cybersecurity measures. Under this, fintech companies will appoint nodal officers to work closely with law enforcement agencies, while banks will demand stricter audits of fintechs' KYC norms due to concerns over non-reporting to credit bureaus.

THE WAY FORWARD

The government should focus on fast-tracking the introduction of a comprehensive data protection law and refining the Digital India Act to better regulate fintech activities. Clear mandates regarding data usage, user consent, and information sharing between fintechs, banks, and law enforcement agencies need to be established. Further, regular audits of KYC norms for fintech companies should be made mandatory, with a uniform standard of reporting to credit bureaus. The RBI may also consider introducing specific guidelines for outsourcing core services to reduce regulatory risks for non-bank lenders. Furthermore, to ensure long-term success, India must align its fintech regulations with global AML standards, such as FATF guidelines. This would not only reduce fraud but also improve India's standing in international financial markets. This collaboration could redefine India's approach to cybersecurity in finance, provided it is backed by a strong legal and regulatory framework.

ARTIFICIAL INTELLIGENCE

SECTION 4

SINGAPORE'S DEEPFAKES LEGISLATION: A DESPERATE MEASURE?

NEWS

In a recent development, Singapore jumped into the bandwagon of curbing the use of Generative AI to spread misinformation in elections. Deepfakes across the world have caused a ruckus in the stainless conclusion of the electoral process.

LEGAL TALK

An amendment proposed for the Presidential Elections Act 1991 creates publication of online election advertising an offence if it's a false representation of something that the candidate in fact did not say or do, but the representation is realistic enough such that it is likely that some members of the general public would, if they heard or saw the representation, reasonably believe that the candidate said or did that thing, where such content was generated either wholly or partially using digital means. An exception to any prosecution under this would be if on a balance of probabilities, that the person did not know and had no reason to believe that the candidate did not in fact say or do the thing. Once a corrective direction is issued, the social media services acting as intermediaries would be tasked with immediate and expedient removal of the content from their platform. The amendment puts more emphasis on this general rule by increasing the punishment for non-compliance up to $ 1,000,000. Ms. Josephine Teo, Minister for Digital Development and Information, while presenting the amendment, pleaded the candidates to be proactive in flagging out such malicious use of technology against them and protect their electoral collections. Recently, the state of California introduced new laws pertaining to regulation of online advertising in elections, *Elections: Deceptive Media in Advertisements Act 2024*, with a similar intent of regulating AI content generated for electoral campaign. An important highlight of that act which seems to be missing from the Singapore legislation is the identification of the election officials as an important stakeholder. The Singapore law and the mechanism it intends to bring only candidates, while election officials are also an imperative organ in the process.

Even other than the election official, the mechanism is restrictive because it does not cover many other scenarios where deepfakes could be used to manipulate the process, e.g. targeting specific groups, stereotyping particular regions as biased, alleged corruption in ballot machines and other general things that might not be true and may hamper public trust in the electoral process. Further, while the Singapore act prescribes regulatory actions by the intermediaries, there is a lacuna in the act's approach to prescribe advisory actions that can be beneficial for people. An example for this can be taken from the Californian legislation which prescribes labelling of content as AI generated by the users. This mandates for intermediaries to be constantly vigilant about AI content circulating on the App and ensures that people can actively distinguish between generated content. Another example that can be followed is that the intermediaries must themselves flag mass reported publications to be potential misinformation.

THE WAY FORWARD

The Singapore legislation is definitely a great stride forwards towards encountering deepfake content, however its only limitation is the limited action approach they have taken. The issue of deepfakes is very extensive and can create unpredictable hindrances, thus it is predicted that a legislation for the same should be proactive in the regard of having a wide reach over all potentially harmful content. The curb should not be limited to the candidates, but ideally should be beneficial for the whole process. That being said, Singapore has had an illustrative history of very effective legislations that are an inspiration for countries to follow and the approach for this legislation might be attributed to the Singapore General Elections just around the corner. It is not far from sight that the Law-makers would soon catch up to counter the threats posed by this technology.

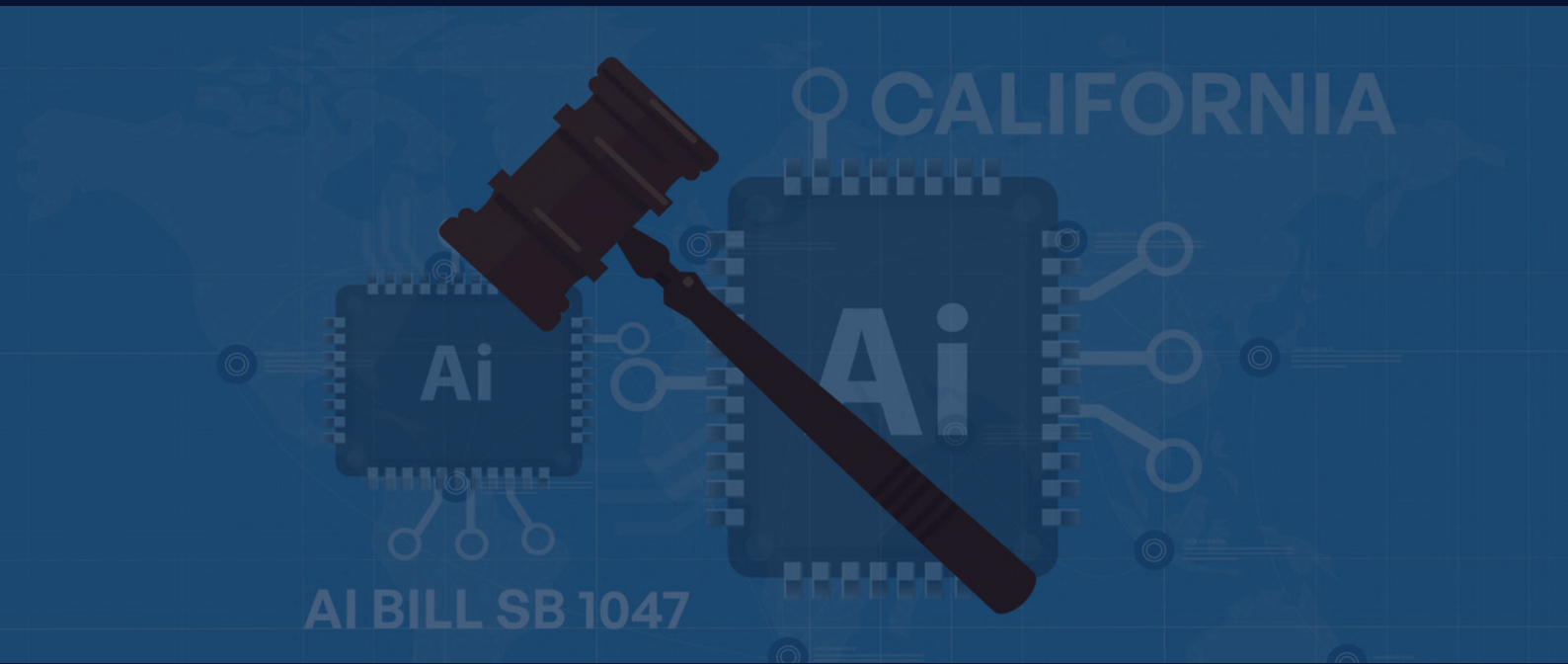
CALIFORNIA GOVERNOR VETOES CONTENTIOUS AI SAFETY BILL

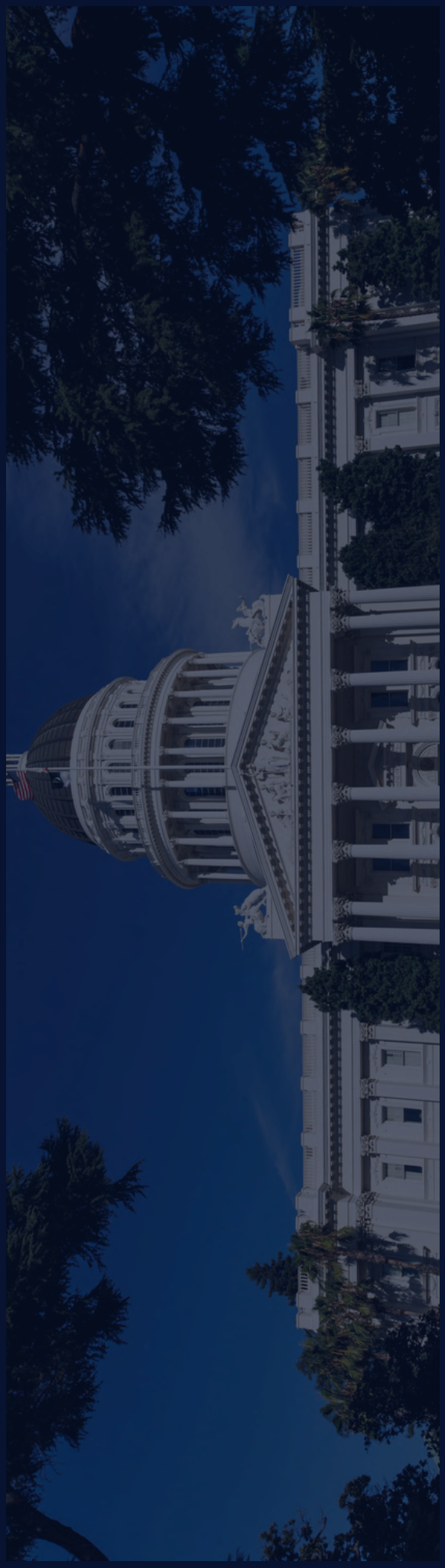
NEWS

California Governor Gavin Newsom vetoed the AI Safety Bill on the grounds that it would drive business out of the state and stifle innovation. The proposed measure required advanced AI models to pass safety tests and be designed with a 'kill switch'. Google, OpenAI, and Meta generally opposed the bill.

LEGAL TALK

The Senate Bill 1047 made it mandatory for the designing of AI models with a 'kill switch' which means that the AI models needed to have a switch to turn it's functioning off when it turns harmful for the safety and security of the public. This is necessary when the AI models have very little human supervision. This mandate was made keeping in mind the problem of cyberattacks and weaponization of AI models but the approach taken by the bill was flawed. The terms of the bill have been criticised for being too vague and ambiguous creating doubts in the minds of the developers as the bill defines AI models as a 'covered AI model' which means the model was either trained by a highly advanced computing power and or it has similar performance to that of a state-of-the-art foundation model. The bill also has the same rules for all AI models regardless of the degree of danger that they can pose. For instance, it imposes the same standards on AI applications used to generate academic content and an AI application used to generate data for research in medicine. This shows that the bill doesn't differentiate between high-risk and low-risk models. The differentiation is required to determine the stringency of the punishments just like how our laws differentiate between crimes committed by a child to that of an adult in terms of the way they would be punished. The bill also discourages open source development because it mandates the developers to produce and retain a redacted copy of the safety and security protocol, including details of updates or revisions made on the AI model to the Attorney General. It also holds the developers responsible for misuse, forgetting that the developers cannot determine the use of criminal-minded offenders. Finally, as proposed by the bill, stiff penalties and ambiguous rules may discourage developers from sharing or publishing their models, hurting transparency and research.





THE WAY FORWARD

The main implication from the bill is that it impacts innovation and treats all AI models as one which is wrong as each AI model is unique in its working and has different purposes. Opponents of the bill have also argued that it restricts open-source initiatives and harms competitiveness. A risk-based approach in the Senate Bill 1047 would overcome the cons. There needs to be regulation that classifies which AI applications are high-risk and which are low-risk, so a developer with less impact or low-risk projects does not have to deal with strict scrutiny. The language in the bill must be clarified by spelling out the criteria for 'unreasonable risk' to eliminate legal uncertainty. It should further aim at moving from full liability on developers to a system of shared responsibility that seeks better understanding of how AI models actually apply downstream. Open-source projects should be exempt or have less stringent requirements to encourage openness and collaboration. Finally, the practicality of the 'kill switch' requirement needs to be reviewed as well because it goes hand in hand with the technical challenges it poses on distributed and decentralized AI models.

DATA PRIVACY

SECTION 5

RTI CONCERNS UNDER DPDPA

NEWS

Recent media reports have revealed that, during the inter-ministerial consultations, NITI Aayog advised the Ministry of Electronics and Information Technology ('**MeITY**') against passing the proposed Digital Personal Data Protection Act ('**DPDPA**') in its current form, citing concerns that it could weaken the Right to Information ('**RTI**') Act.

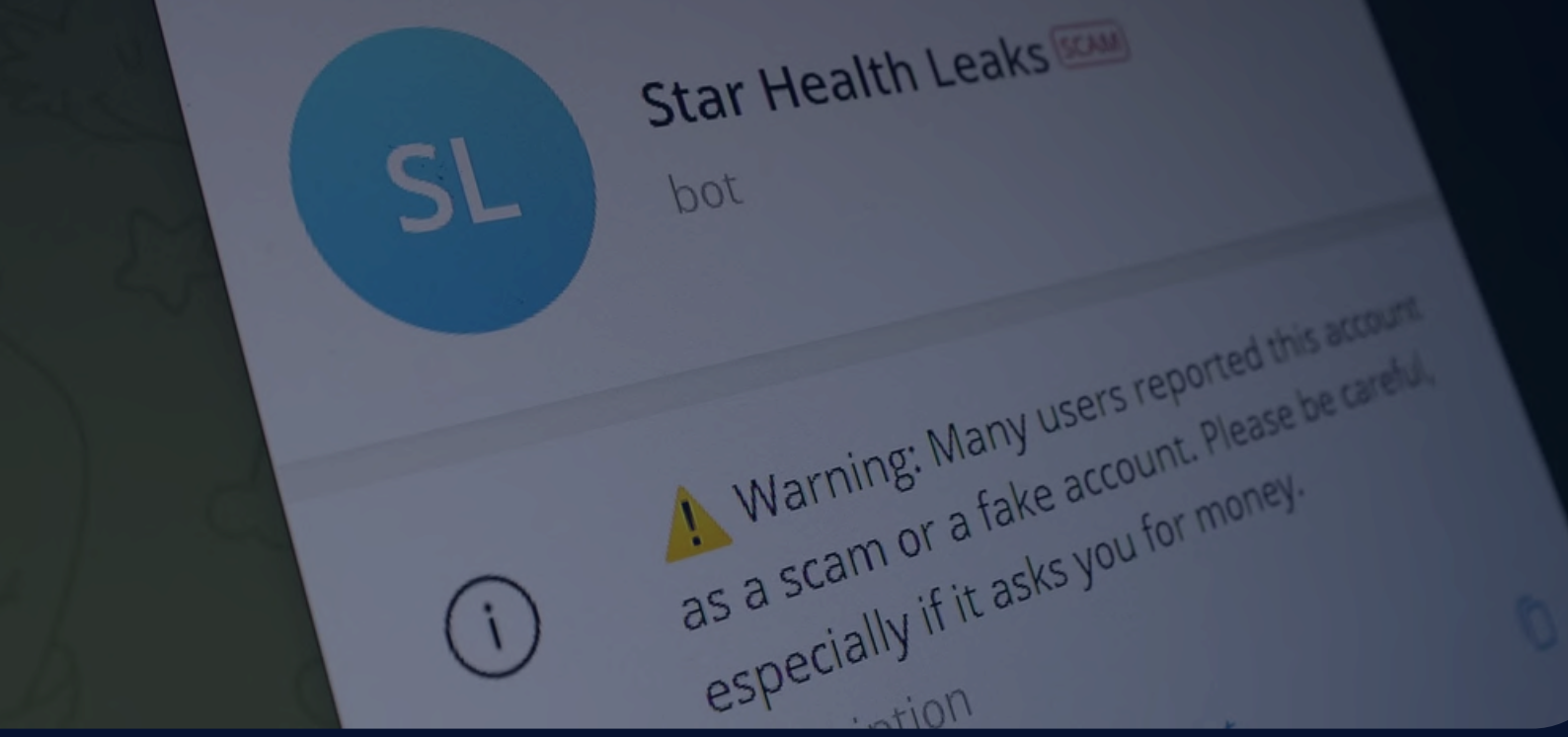
LEGAL TALK

The key issue centres around an amendment to Section 8(1)(j) of the RTI Act. This section currently restricts public authorities from sharing personal information on two grounds: if the disclosure has no relevance to any public activity or if it would lead to an unwarranted invasion of an individual's privacy, unless the disclosure is justified by a larger public interest. Under Section 44(3) of the DPDPA, this clause would be replaced with: "information which relates to personal information." The change would remove the earlier provision that allowed relevant officials to disclose personal information if they determined that doing so was in the larger public interest. NITI Aayog argued that this revision would strip Public Information Officers of the discretion to assess the public interest, which has been a crucial part of the RTI framework. It would undermine the public's access to information, as it would prevent authorities from disclosing personal information even when it could hold significant public value. Also, anyone seeking information through the RTI Act about official documents could find themselves falling within the definition of 'personal information'. The issue then arises from the DPDPA's expansive definition of a 'person', which includes not only individuals but also entities such as Hindu undivided families, companies, etc. With such an inclusive definition, any information related to these entities could be classified as 'personal information', potentially allowing authorities to deny access to critical information under the guise of protecting privacy. The government argued that the right to privacy, recognized as a fundamental right under the Constitution of India, should also extend to officers in government institutions. However, this perspective appears somewhat unnecessary because, while the right to privacy existed under the previous provision, albeit not in an absolute form, it struck a balance between protecting individual privacy and promoting transparency.

It allowed officials to withhold information if it could lead to an unwarranted invasion of privacy, a condition broad enough to enable them to exercise their discretion. Simultaneously, wide discretionary powers were granted to officials, which carries the risk of misuse. The lack of a precise legal definition of 'personal information' further expanded this discretion. Both approaches—retaining discretion or removing it—have their advantages and disadvantages, making it a complex issue. The key question is where the cost-benefit analysis tilts. In the scenario where no such amendment is made, officials would still have discretionary powers, but in cases of doubt, the presumption could lean toward disclosure in the interest of the greater public good. The onus would be on proving that disclosing personal information was not justified. This system could have helped achieve a reasonable balance between protecting the state's interests and the individual's privacy while also safeguarding the public's right to information. However, the new amendment removes this option altogether. By prioritising privacy over transparency, it weakens the right to information. The status quo offered a middle ground where both rights were reasonably balanced. It is pertinent to note that Section 8(2) of the RTI Act remains untouched by the draft DPDP Bill. This provision allows a public authority to disclose requested information if it determines that public interest outweighs the potential harms to protected interests. As a result, individuals could still petition for disclosure under the RTI Act, even after the amendment, using Section 8(2) as a basis. However, it may be overly optimistic to depend on this to mitigate the likely rise in RTI denials following the amendment. While the section provides a mechanism to argue for the release of information in the public interest, it may not fully offset the broader impacts of the amendment.

THE WAY FORWARD

Despite objections from NITI Aayog, MeitY kept the changes intact. This raises serious concerns, as access to personal data is crucial for holding governments accountable in a democracy. In the absence of such publicly accessible personal data, it is impossible for intended beneficiaries to access their rightful entitlements and benefits. The RTI Act has been instrumental in protecting citizens' rights, and the new privacy law should clearly state that disclosing personal data for public interest does not violate privacy. Without solid evidence showing that public interest harms privacy, this decision is likely to cause more harm than good.



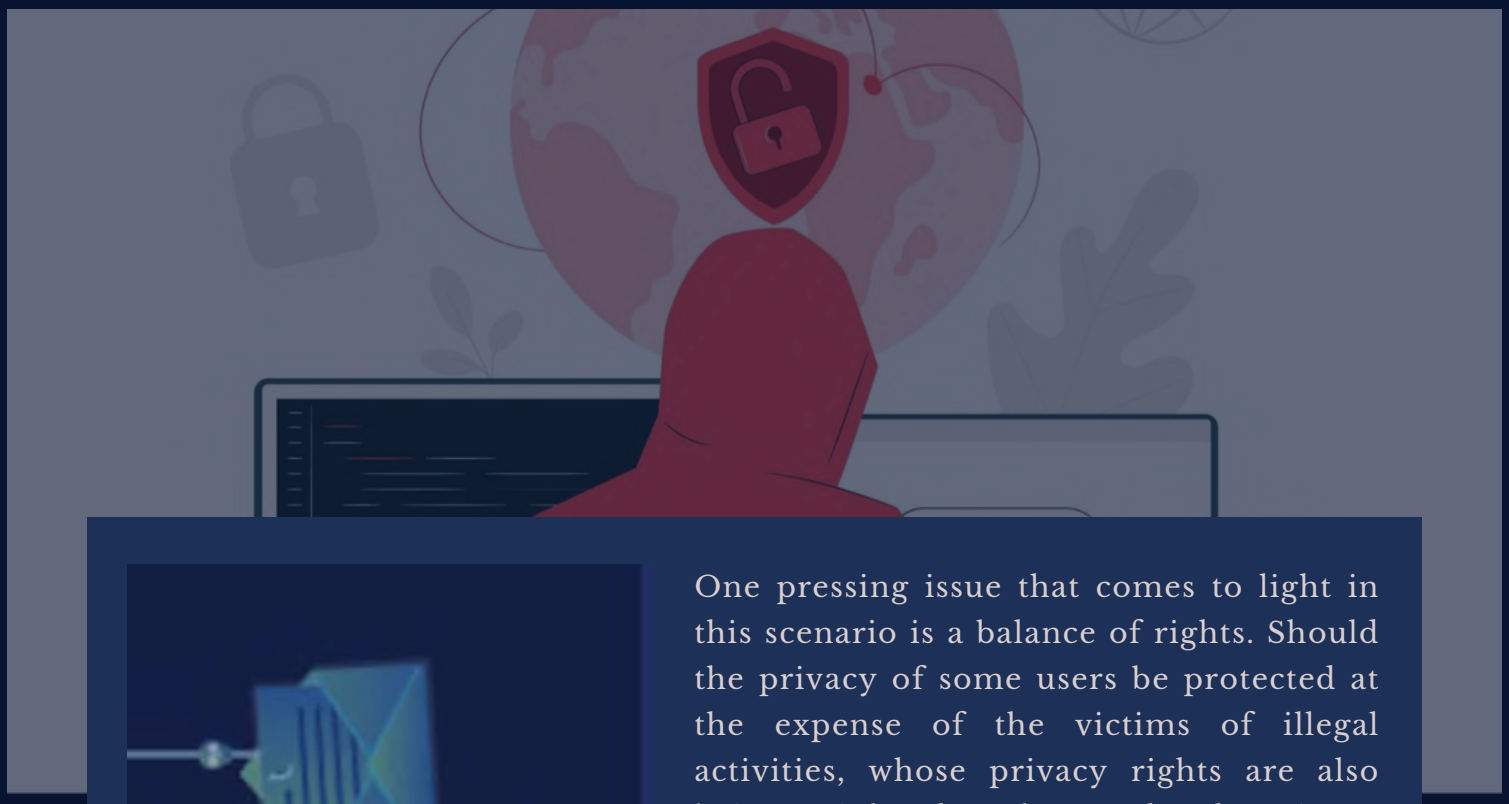
STAR HEALTH INSURANCE SUES TELEGRAM OVER PERSONAL DATA LEAK OF 3 CRORE CUSTOMERS

NEWS

Star Health Insurance has sued messaging platform Telegram as sensitive personal data of about 3.1 crore customers was leaked by a hacker identified as xenZen, using chatbots on the platform. This has come just weeks after Telegram founder Pavel Durov was accused of allowing the app to facilitate crime and the recent changes to its privacy policy. The leaked data includes policy and claims documents featuring names, phone numbers, addresses, tax details, copies of ID cards, test results and medical diagnoses. The Madras High Court has issued a temporary injunction directing Telegram to block access to compromised data made available through chatbots and websites.

LEGAL TALK

As per the Digital Personal Data Protection Act, 2023 ('**DPDPA**'), personal data can only be processed for certain legitimate uses specified in Section 7. These include disclosure of personal data for fulfilling obligations under any other law in force at the time as well as complying with a court order under sub-sections (d) and (e) respectively. Telegram has been adamant about non-disclosure of data to authorities claiming that it cannot compromise on its encryption. Mass communication features, ability to store and share large amounts of data through anonymous accounts and creation of customizable chatbots make the platform a breeding ground for exchanging child sex abuse media, terror-related content, and misinformation. This also raises issues in the light of Section 3(b) of the Information Technology Rules, 2021, which requires intermediaries to make reasonable efforts to not host such information on their platforms.



One pressing issue that comes to light in this scenario is a balance of rights. Should the privacy of some users be protected at the expense of the victims of illegal activities, whose privacy rights are also being violated? The updated privacy policy states that if Telegram receives a court order confirming that a user is suspected of engaging in criminal activities that violate its Terms of Service, the company will conduct an internal investigation and may disclose user data to the authorities. Such instances are proposed to be published in its quarterly transparency report. This showcases a notable shift as Telegram will now provide authorities with user data including phone numbers and IP addresses, in response to 'valid legal requests'. However, it has made sure that it exercises the majority of discretion by using words such as 'may' and 'valid legal requests' in the privacy policy, thus raising doubts over this measure and its future standpoint on compliance with the law.

THE WAY FORWARD

The ability of hackers to exploit Telegram chatbots to sell stolen data emphasises the platform's vulnerability to malicious activity. While the right to privacy is fundamental to the very existence of an individual in society, it is not an unfettered right. Platforms like Telegram act as Data Fiduciaries and social media intermediaries at the same time. Therefore it is imperative for them to ensure compliance with both frameworks. The enforcement of the DPDPA and the proposed Digital India Act can play a crucial role in this respect.

CONTRIBUTORS

WRITERS

MAITHILI DUBEY
PRATYUSH SINGH
ARUNIMA RAMAN
KALYANI KIRAN
SUBHASIS SAHOO
SATVIK MITTAL
ARUNIMA RAMAN
ALOK SINGH MOURYA
BHAVYA BHASKAR
TRISHNA AGRAWALLA
ANUSHKA GUHA

EDITORS

HARSH MITTAL
LAVANYA CHETWANI

DESIGNERS

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL