SALOT & SHAH ASSOCIATES

NEWSLETTER

JUNE 2024

INTRODUCTION:

Welcome to the Digital Navigator, your go-to source for navigating the ever-evolving landscape of digitalization. Explore the latest trends, breakthroughs, and insights shaping our digital frontier. Reconnoitre on a journey through the cutting-edge realms of technology, innovation, and digital transformation.

More Info

www.salotandshah.com

info@salotandshah.com

+91 - 93286 69060

DIGITAL INDIA ACT, 2023 (DIA): Comprehensive Framework for Regulating the Digital Landscape

INTRODUCTION:

In a landmark development, the government has introduced the Digital India Act 2023 ("DIA"), signalling a significant shift in the regulatory landscape for the digital industry. Envisioned as a comprehensive replacement for the Information Technology Act of 2022, the DIA is designed to curb market power concentration and gatekeeping practices by big tech companies. This legislative initiative aims to foster choice, competition, fair market access, and ease of doing business in the rapidly evolving digital space.

REVAMPING SAFE HARBOUR PROTECTIONS

There is a comprehensive legislation is poised to potentially serve as the foundational document.

Reports suggest that the Digital India Act 2023 is set to oversee a range of operations, including data localization, social media activities, online gaming, the prevention of cyberbullying, e-commerce practices, regulations of artificial intelligence, and the oversight of internet platforms.

One of the key areas of scrutiny under the DIA is the revisitation of safe harbour protection granted to intermediaries, currently governed by the Information Technology Act's safe harbour provision. The Ministry of Electronics and Information Technology ("MeitY") emphasized on the urgent need for a specialized and dedicated adjudicatory mechanism for online civil and criminal offences.

This move reflects the government's commitment to re-evaluate the balance between providing a conducive environment for digital intermediaries and ensuring accountability for their actions. Striking the right balance is crucial for promoting innovation while safeguarding the interests of users and stakeholders.`

ESSENTIAL ACCESS TO GOVERNMENT & PUBLIC UTILITIES

A fundamental objective of the DIA is to ensure essential access to government services and public utilities in the digital governance sphere.

Another objective is to formulate evolvable rules that are consistent with the changing trends in technologies and can be updated according to the needs of the country's infrastructure.

By incorporating provisions that mandate streamlined access to crucial services, the act aims to bridge the digital divide and enhance the inclusivity of digital governance.

This step aligns with the government's vision of leveraging technology to create a more accessible and efficient public service delivery system.

REGULATING THE DIGITAL INDUSTRY

The DIA casts a wide regulatory net, covering various facets of the digital industry. This includes social media companies, e-commerce platforms, search engines, gaming, telecom providers, over-the-top (OTT) platforms, artificial intelligence, etc. The expansive scope of the DIA reflects the government's recognition of the interconnected nature of digital services and the need for a unified regulatory framework to address diverse challenges.

PROTECTING MINORS & ENSURING ETHICAL TECH USE

Addressing concerns related to the impact of technology on minors, the DIA includes provisions aimed at protecting them from addictive technology. Recognizing the need for a balanced approach, the act seeks to establish safeguards to prevent the exploitation of vulnerable demographics.

Additionally, the DIA introduces the right to be forgotten, providing individuals with greater control over their digital footprint and personal data.

TACKLING MIS-INFORMATION ON SOCIAL MEDIA

Fake news and misinformation have become pervasive issues in the digital age. Social media platforms will be subject to measures aimed at moderating the spread of the fake news, ensuring responsible content dissemination, and mitigating the potential societal impact of the mis-information. These provisions currently underscores the government's commitment to fostering a digital environment that prioritizes accuracy and accountability.

DEFINING & REGULATING AI AND WEARABLES

In a forward-looking move, the DIA takes a proactive stance on emerging technologies by defining and regulating AI and wearables. By establishing clear guidelines and standards for these technologies, the government aims to promote responsible development and use. Ensuring accountability and transparency of algorithms is a crucial aspect of this regulatory framework, reflecting a commitment to ethical AI practices.

AMENDMENTS TO THE COMPETITION ACT OF INDIA

Recognizing the evolving nature of the digital landscape and the potential for market distortions, the DIA mandates amendments to the Competition Act. This strategic move aims to equip regulatory authorities with the necessary tools to address anticompetitive practices and ensure a level playing field. The amendments signal the government's responsiveness to the dynamic challenges posed by digital markets and its commitment to fostering healthy competition.

ESTABLISHMENT OF AN ADJUDICATOR & APPELLATE MECHANISM

To enforce the provisions of the DIA and hold big tech companies accountable for any breaches, the legislation proposes the establishment of an adjudicator and appellate mechanism. This signifies a departure from traditional regulatory approach, and emphasize on a specialized framework which is dedicated to addressing the unique challenges posed by the digital industry. This mechanism aims to provide timely and effective resolution of the disputes, contributing to the overall efficacy of the regulatory framework.

ADDRESSING CONCERNS OVER BIG TECH COMPANIES

The government's decision to regulate the digital industry comes against the backdrop of growing concerns over the dominance of big tech companies and allegations of their manipulation of the system.

The DIA is positioned as a proactive response to these concerns, with the overarching goal of levelling the playing field and fostering a fair and competitive environment for all participants in the digital space.

CONCLUSION

The introduction of the Digital India Act marks a watershed moment in the regulation of the digital industry. By encompassing a wide array of issues, from revisiting safe harbour protections to defining AI and wearables, the DIA reflects a comprehensive and forward-looking approach to digital governance.

As the digital landscape continues to evolve, the DIA positions India as a trailblazer in adapting its regulatory framework to meet the challenges and opportunities presented by the digital era. Through this legislative initiative, the government aims not only to address existing concerns but also to lay the foundation for a resilient and inclusive digital ecosystem that prioritizes the interests of users, fosters innovation, and ensures fair competition.

NAVIGATING THE DYNAMICS OF DIGITAL CONSENT ACQUISITION: A Closer Look at TRAI Mandate

INTRODUCTION:

In the ever-evolving realm of digital communication and services, the focal point has shifted to user consent, prompting global regulatory bodies to institute guidelines safeguarding individual privacy and data. Within India, the Telecom Regulatory Authority of India ("TRAI") has played a pivotal role in shaping the landscape of digital consent acquisition through its mandate. This article explores the intricacies of digital consent, the TRAI mandate, and its implications for both consumers and businesses. In a bid to combat the proliferation of unsolicited commercial messages, TRAI issued a directive on October 2, 2023, under the Telecom Commercial Communication Customer Preference Regulation, 2018 ("TCCCPR").

In the conventional system, user consent records were managed independently by various entities, posing a significant challenge for access providers (APs) to verify their authenticity.

Recognizing this complexity, the Digital Consent Acquisition System was introduced to streamline the process, offering APs a more efficient means to monitor and authenticate user consent records, thereby facilitating the smooth transmission of the commercial communication.

The previous approach to tracking user consent was decentralized, with principal entities managing consent records separately. This fragmented approach presented challenges for access providers in validating the legitimacy of consent records. To address these issues, the Digital Consent Acquisition System was implemented to simplify and centralize the management of user consent.

AIM OF INTRODUCING DIGITAL ACQUISITION SYSTEM

This system aims to provide access providers with a more effective mechanism for overseeing and validating user consent. By consolidating consent records, it not only enhances accuracy and reliability of the information but also ensures a smoother process for access providers.

This streamlined approach not only addresses the challenges of the past system but also facilitates the secure and efficient transmission of commercial communications based on the verified and authenticated user consent records.

Digital consent pertains to the explicit permission granted by individuals for the collection, processing, and storage of their personal information. With the proliferation of digital services, ranging from mobile applications to online platforms, the necessity for clear and informed consent has become paramount. Users must be cognizant of how their data will be utilized, ensuring proper transparency and control over their personal information.

The entire Digital Consent Acquisition (DCA) facility revolves around the consent-seeking messages sent to users by principal entities (PEs) with the assistance of access providers. PEs are mandated to compile a list of authorized URLs, APKs, OTT links, and call-back numbers for use in consent-seeking messages, preventing unauthorized access or misuse of customer data. If a customer does not respond or rejects the message, the PE cannot resend it for the next 90 days. However, customers retain the right to initiate consent registration at any time, shielding them from unwarranted communication by PEs.

TIMELINE FOR THE DCS IMPLEMENTATIONS

The process of PE-initiated consent acquisition should commence one month after the full functionality and advertisement of the DCA Facility or 30 days after its successful implementation. Until then, customer-initiated consent registration can occur. Successful DCA implementation is declared when it is fully functional, and PEs have initiated consent registration through consent-seeking messages. As per TRAI's timeline, PE-initiated consent acquisition was set to commence from September 1, 2023. After this date, PEs cannot use previously acquired consent and must adhere to the DCA process to obtain fresh consent.

The on boarding of PEs belonging to the banking, insurance, finance, and trading sectors is prioritized, followed by other sectors. This prioritization is influenced by the stringent regulatory requirements and complexity within these industries, requiring meticulous integration processes to ensure compliance.

Addressing the intricacies of these sectors first allows for a focused and comprehensive approach, reducing the risk of non-compliance and ensuring a smoother transition for industries governed by rigorous regulatory frameworks.

IMPLICATION OF NEW & IMPROVED CONSENT COLLECTION

The directive stipulates that existing consents obtained through other means will become null and void, rendering any previous consents obtained through non-digital methods invalid. PEs must seek fresh consents exclusively through the DCA process with the aid of access providers. Transitioning to a standardized DCA process promotes consistency in data collection methods, offering enhanced security measures and a verifiable platform for access providers to track consents.

By nullifying the non-standardized consents and acquiring fresh consent through a standardized digital process, TRAI aims to intake only valid and compliant consents for advertising purposes. This marks the end of arbitrary methods employed by PEs for sending advertisements, ensuring a more regulated and accountable approach.

THE AFTER EFFECTS

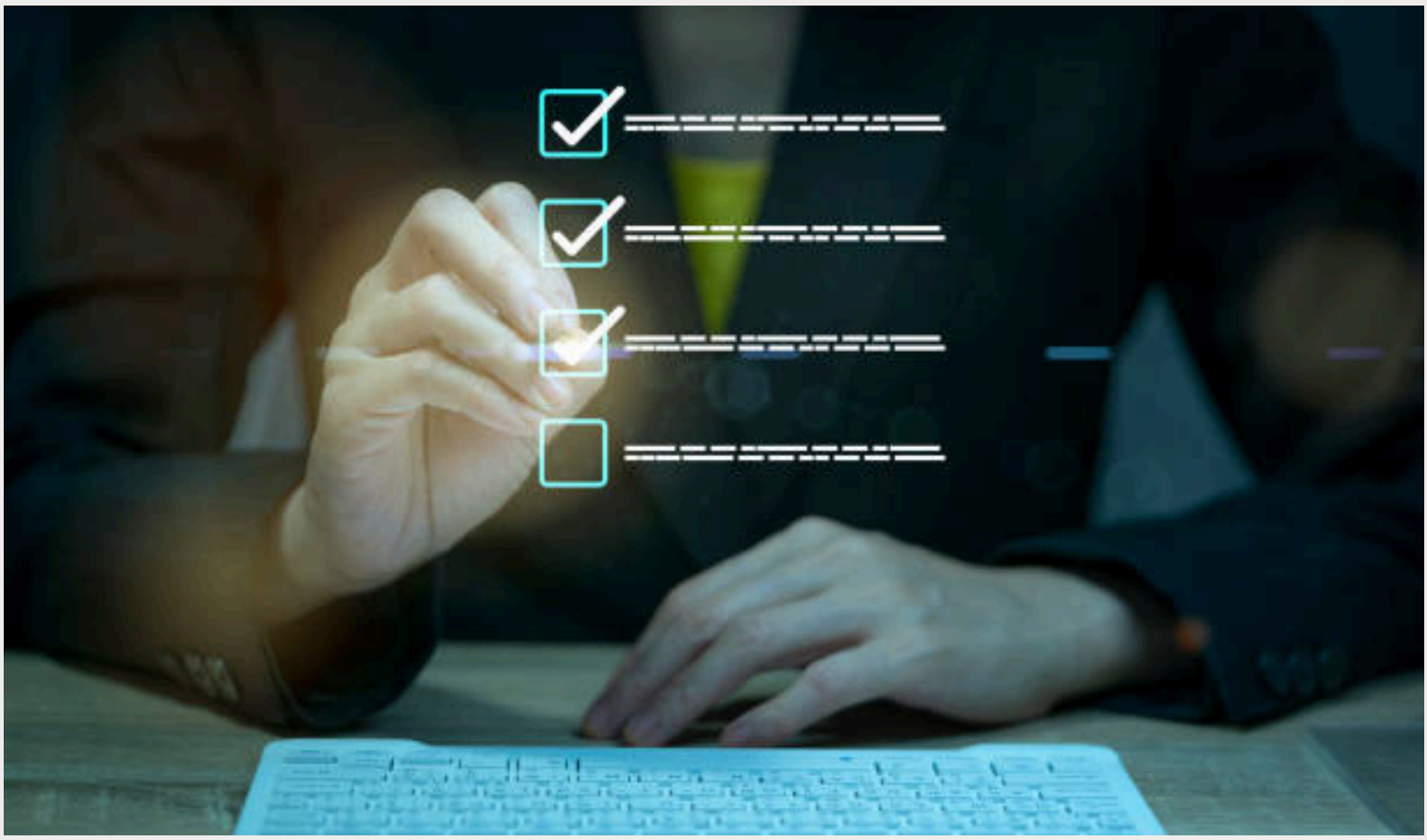
The implementation of the Digital Consent Acquisition (DCA) facility will have significant ramifications on the relationships between Access Providers (APs), Principal Entities (PEs), and users. While it grants users greater control over the messages they receive, it places a substantial burden on PEs, requiring them to individually obtain consent from each user—a potentially difficult task. Users now have the formal ability to select which commercials they wish to receive and avoid those they consider unwanted or spam, placing the responsibility on PEs to convincingly engage users for their consent.

APs must collaborate not only with PEs but also with users to ensure the seamless functioning of this new system.

Sustaining scalability amidst fluctuating or expanding user numbers demands ongoing attention to uphold adaptability. The technical integration process entails intricate modifications to existing systems, involving meticulous adjustments to databases and software interfaces. Training staff to navigate the new process and supporting users unfamiliar with the digital consent system necessitate allocating resources for training programs and continuous user assistance, thereby adding to the operational burden of access providers. Furthermore, the guidelines stipulate that APs must educate PEs on the intricacies of the new process.

CONCLUSION

Although the DCA system may pose challenges for both PEs and APs, yet it signifies a necessary change. It further elevates the transparency as well as the accountability in the consent process, shielding users from unsolicited advertisements. APs must collaborate with PEs to gather necessary information and adhere to TCCCPR's regulatory standards. Therefore, the DCA provides a standardized and digitally verifiable process for acquiring consent, safeguarding the privacy and preferences of users.



THE DIGITAL FRONTIER: India's Cyber Security Imperitive in the Era of Rapid Transformation

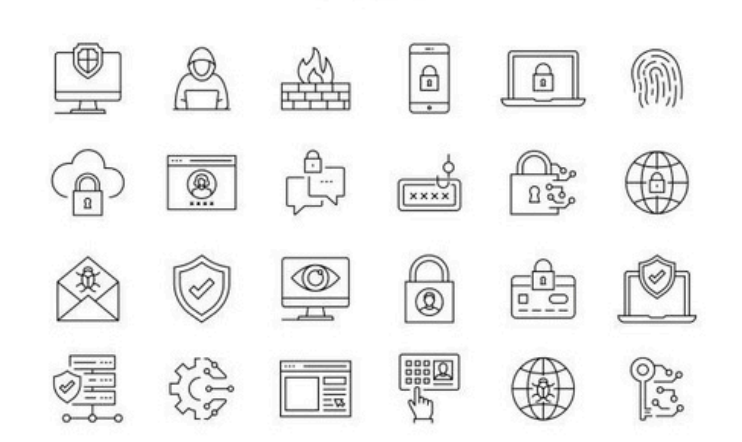
INTRODUCTION:

In the wake of India's rapid digital transformation and the proliferation of advanced technologies, the country finds itself at the forefront of a technological revolution. However, this surge in innovation comes hand in hand with the burgeoning concern over the security of vast data repositories. Cybersecurity experts, gathering at the Singapore Cyber Week 2023, have raised alarm bells about the monumental challenge of safeguarding data in the face of both neighbouring adversaries and the escalating sophistication of cybercriminals. This article explores the current cybersecurity landscape in India, the industries most affected by cyber threats, and the imperative for collaborative efforts to create a robust cybersecurity ecosystem.

THE DIGITAL TANSFORMATION LANDSCAPE IN INDIA

India has witnessed an unprecedented digital boom in recent years, with the government pushing initiatives such as Digital India. These initiatives are taken to transform the nation into a digitally empowered society and knowledge economy. As a result, the adoption of advanced technologies, including artificial intelligence, cloud computing, and the Internet of Things ("IoT"), has surged across industries, paving the way for increased efficiency, connectivity, and innovation.

However, this digital renaissance has not come without its challenges. One of the foremost concerns is the security of the colossal amount of data generated and managed in the country. The ever-expanding attack surface, combined with the geopolitical context and the evolving tactics of cyber adversaries, has propelled cybersecurity to the forefront of national priorities.



THE THREAT LANSCAPE

At the heart of the cybersecurity discourse in India lies the unsettling reality of a continuously evolving threat landscape. According to recent findings from Check Point's Threat Intelligence Report, the country has experienced a significant spike in cyber-attacks over the past six months. On average, each organization in India faced a staggering 2,157 attacks per week, compared to the global average of 1,139 attacks per organization.

The three industries most impacted in terms of weekly attacks per organization were Healthcare, Education/Research, and Utilities. This underscores the multifaceted nature of cyber threats, affecting critical sectors that play pivotal roles in the nation's well-being. Retail, hospitality, manufacturing, and transportation sectors were also identified as potential targets, necessitating swift action to fortify their cybersecurity defences.

COLLABORATION & COOPERATION: THE NEED OF THE HOUR

Against this backdrop of escalating cyber threats, experts unanimously advocate for a collaborative and cooperative approach to cybersecurity. During the Singapore Cyber Week discussions, the consensus was clear – Indian technologists, business executives, and government entities must unite to create a comprehensive ecosystem capable of tackling tech-driven threats effectively.

Mr. Vivek Gullapalli, Chief Information Security Officer, APAC at Check Point Software Technologies, emphasized the complexity of contemporary cybersecurity challenges. He noted that cybersecurity is often left solely to the responsibility of a company's IT team, which may struggle to keep up with the rapidly evolving threat landscape. To address this, a holistic and collaborative effort involving various stakeholders is imperative.

BUILDING A ROBUST CYBER SECURITY ECOSYSTEM

1. **Public-Private Partnerships:**

Establishing strong public-private partnerships is fundamental to fortifying India's cyber security defences. The government, industry leaders, and cybersecurity experts should collaborate to share threat intelligence, best practices, and resources. This collaborative approach will enhance the collective resilience against cyber threats.

2. **Investment in Cyber Security Infrastructure:**

The government and private sector alike must invest in robust cybersecurity infrastructure. This includes the development of advanced threat detection systems, secure cloud platforms, and cutting-edge encryption technologies. Allocating resources to research and development in cybersecurity will be crucial to stay ahead of evolving threats.

3. **Skill Development and Training:**

A skilled workforce is the backbone of any effective cybersecurity strategy. India must focus on fostering a talent pool equipped with the latest cybersecurity skills. This involves investing in training programs, certifications, and educational initiatives to nurture a cadre of cybersecurity professionals capable of addressing the dynamic threat landscape.

4. **Regulatory Framework and Compliance:**

Implementing and enforcing a comprehensive regulatory framework is essential to ensure that organizations adhere to cyber security best practices. Compliance standards should be regularly updated to reflect the evolving threat landscape, and non-compliance should incur significant consequences. This will incentivize organizations to prioritize cyber security measures.

5. **International Collaboration:**

Given the global nature of cyber threats, India should actively engage in international collaborations on cyber security. This involves sharing threat intelligence with other nations, participating in joint cyber security exercises, and contributing to the development of international norms and standards for cyber security.

THE URGENCY FOR THE ACTION

As India hurtles forward in its digital journey, the urgency to address cybersecurity concerns cannot be overstated. The interconnectedness of systems, the proliferation of IoT devices, and the increasing sophistication of cyber threats demand a proactive and collaborative response. The retail, hospitality, manufacturing, and transportation sectors were also identified as potential targets, indicating that the scope of the cybersecurity challenge is broad and affects every facet of the economy. The consequences of a large-scale cyber-attack on critical infrastructure or sensitive data could be devastating, making it imperative for businesses and government entities to act swiftly.

CONCLUSION

In conclusion, India stands at a critical juncture in its technological evolution, where the benefits of digital transformation coexist with the perils of an increasingly complex cyber security landscape. The key to navigating this digital frontier lies in collaborative efforts, proactive investments in cyber security infrastructure, and a concerted focus on skill development.

The recent revelations from the Singapore Cyber Week underscore the need for a comprehensive and agile cyber security strategy. By fostering public-private partnerships, investing in advanced technologies, and prioritizing the development of a skilled cyber security workforce, India can build a resilient cyber security ecosystem capable of withstanding the evolving threats of the digital age. The time to act is now, for the safeguarding of India's digital future depends on the collective commitment to cyber security excellence.

DISCLAIMER

The articles in the newsletter are analyzed as per the personal views of the author and does not reflect the firm's opinion. The newsletter disclaims any views / opinions that readers' may infer post reading thish newsletter; readers' discretion is advised.