SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

International Centre
for Information
Systems and Audit

9th Edition, e-Journal

PursuIT

DATA PROTECTION AND DATA PRIVACY

By International Centre for Information Systems & Audit

Contents

About the Journal

PursuIT, the e-Journal, is a platform for sharing of experience and inculcating professional excellence in the emerging areas in the domain of Information Technology. e-Journal aims at having features on emerging areas of Information Technology viz. cybersecurity, Data Security, e-Governance etc. It also looks into the technological developments, future of technology, national policies and standards, as well as articles on IT Audit conducted by SAI India.

Editorial Board

Ms. Geeta Menon	Additional Dy. CAG & Director General, iCISA
Mr. K S G Narayan	Principal Accountant General (A&E) Assam
Mr. J R Inamdar	Principal Director, iCISA

Feedback/Suggestions

We strive for constant improvement and encourage our readers to provide their valuable feedback/suggestions to make the endeavor successful. Send us your suggestions, comments, and questions about the e-Journal to icisa@cag.gov.in

Disclaimer

Facts and opinions in articles of the e-Journal are solely the personal statements of respective authors and they do not in any way represent the official position of Indian Audit and Accounts Department. This e-Journal is for internal circulation within Indian Audit and Accounts Department only. The contents of this e-Journal are meant for information purpose only. iCISA disclaims all liability for actions taken or failed to be taken based on any content of this e-Journal.

Submission of Articles

To support this initiative of e-Journal, we welcome you to contribute electronic submission of articles from emerging areas in the domain of Information Technology. The article should be relevant to the theme of the upcoming e-Journal and should be in the range of 1000 to 3000 words. All submissions should be accompanied by a short profile of the author. The article is to be sent icisa@cag.gov.in

Director General's Message

Welcome to the ninth issue of PursuIT, the e-Journal of iCISA. As we navigate the evolving landscape of information technology auditing, we remain dedicated to exploring new avenues, particularly in the critical areas of data privacy and data protection. Our goal is to broaden the knowledge base of IA&AD personnel while fostering a culture of experience sharing.

This issue delves into contemporary IT concerns, with a special focus on the challenges and best practices surrounding data privacy and protection. We hope it sparks your interest and enhances your understanding of these vital topics.

I extend my heartfelt gratitude to the authors and the members of the Editorial Board. Your efforts make PursuIT a valuable resource. As we continuously strive to improve and adapt to the ever-changing digital landscape, I encourage our readers to share their insights and suggestions for future editions.

Thank you for your continued support.

Ms. Geeta Menon
Additional Deputy CAG & Director General, iCISA

The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government

By Sh. Manoj Roy Sarkar, AAO, O/o AG(Au) Assam

Mr. Manoj Roy Sarkar is currently working as Assistant Audit Officer in AMG-II section of the O/o the AG(Audit), Assam. He belongs to Civil Audit Cadre with experience in Performance, Compliance, Certification Audits. He also has the experience of auditing the computerized billing system of APDCL, Assam, which was based on the SAP platform.

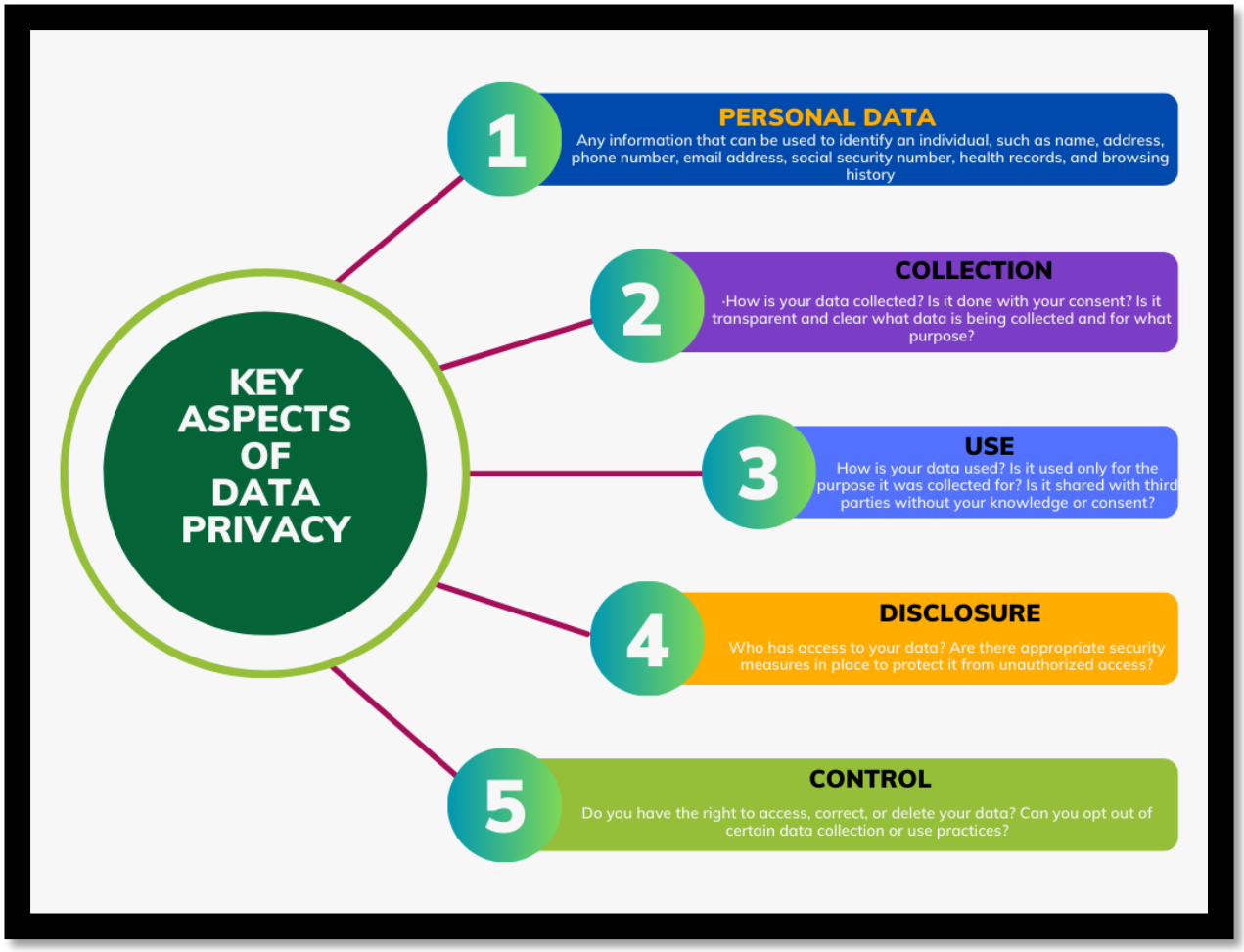
The article discusses India's digital transformation and the challenges of data privacy amid rapid technological innovation. It highlights the importance of protecting personal information, particularly with the implementation of the Digital Personal Data Protection (DPDP) Act, 2023. The text addresses concern such as identity theft, discrimination, and government surveillance while outlining the evolving threats to digital privacy.

India, with its billion-plus population and a thriving digital ecosystem, stands at the forefront of technological innovation. The rapid growth and accessibility of data has transformed the way of Government's operation, revolutionising up its public services and driving unprecedented levels of innovation for its citizens. With its rapidly growing digital population and ambitious initiatives like Digital India, the Government stands at a critical juncture regarding data privacy. Balancing the need for innovation and efficiency with the fundamental right to privacy enshrined in the 2017 Supreme Court judgment[1] has become a pressing challenge. As technology continues to evolve and shape our lives, it is crucial that we understand the importance of data privacy and the ethical responsibilities that come with it.

(A). What is Data Privacy?

Data privacy refers to the protection of personal information, ensuring that individuals have control over how their data is collected, processed, stored, and shared. It encompasses the right of individuals to keep their information private and secure, limiting unauthorized access or use by others.

"Data privacy" usually refers to the handling of critical personal information, also called "personally identifiable information" (PII). This information can include social security numbers, health records, and financial data, including bank account and credit card numbers. In a business context, data privacy goes beyond the PII of employees and customers. This could involve things like proprietary research, development data, or financial information.



(B.) Why data privacy is so important?

i. **Protection against identity theft and fraud:**

Sharing personal information can leave you vulnerable to identity theft and financial fraud. Identity theft is when cybercriminals illegally access personal and critical information about an individual and compromise the same with ulterior motives, which includes siphoning off money from bank accounts or creating fake social-media profiles and taking control of accounts for personal vengeance.

ii. **Protection against discrimination:**

Data can be used intentionally for personal gain to discriminate against individuals based on the factors like race, religion, or political beliefs leading to instability of social & political ecosystem of a country.

iii. **Transparency and accountability:**

Popular digital platforms and mobile apps collect extensive amounts of user data to offer personalized experiences,

targeted advertising, and optimized services but never fully disclose its uses to its users. Similarly, location-based services enhance navigation and provide recommendations but track users' movements, compromising their privacy.

iv. **Data driven innovation and economic growth:**

Protecting individual privacy while fostering data driven innovation can lead to the development of new technologies and services that benefit society as a whole.

Example: M-Pesa[2] in Kenya, a mobile money transfer service, facilitated financial inclusion for millions who lacked access to traditional banking services by utilizing mobile phone data and alternative credit scoring methods allows previously excluded individuals access to financial services like loans and insurance. Similarly, the UK Biobank[3], a large-scale biomedical database, facilitates research on various diseases and contributes to advancements in preventative care by studying its population health database. It is important to remember that these advancements often rely on anonymized or aggregated data to minimize privacy risks.

v. **Protection against Government Surveillance:**

Sometimes Government surveillance threatens individual privacy by undermining the principles of consent, transparency, and proportionality. It can create a chilling effect on free expression and association, as individuals may fear repercussions for expressing dissenting opinions or engaging in activities that are perfectly legal but perceived as threatening by authorities.

Example: The revelations by Edward Snowden in 2013 exposed the U.S. National Security Agency's (NSA) mass surveillance programs, such as PRISM[4], which collected data from major tech companies, collected metadata on millions of Verizon customers' phone calls, highlighting the extent to which Governments can track citizens' communications without their knowledge, raising concerns about global privacy violations.

(C.) How Government Department's data is stored in India -

Government departments in India typically utilize cloud storage services offered by authorized private companies to manage extensive data. Cloud computing allows users to rent or utilize software, storage, and servers as needed, eliminating the necessity to invest in an entire system. The Ministry of Electronics and Information Technology (MEITY)[5] has enlisted the services of 11 private companies to deliver cloud computing services to Government departments. This approach empowers Government entities to scale their IT infrastructure based on demand, even for short durations, facilitating the prompt launch of online services. The cloud computing guidelines adhere to the Megh-Raj Policy (cloud policy), offering a strategic framework for the government's adoption of cloud services. The overarching goal of the cloud policy is to materialize a comprehensive vision of a Government Cloud (GI Cloud) environment, accessible to central and state Government's line departments, districts, and municipalities. This initiative aims to expedite the enhancement of ICT-enabled services across Government entities.

(D.) Evolving Threats to Digital Privacy in India: -

The digitalization wave in India has been transformative, with technologies such as Aadhaar, e-Governance, and digital payment systems like UPI reshaping Government operations. Government organizations embrace digital transformation to enhance public services, streamline operations, and engage with citizens. While digitization of various Government services promising greater efficiency, raise concerns about the security and privacy of citizens' data misuse and potential violation of privacy rights.

Here are some of the evolving threats to digital privacy in India-

i. **Cybersecurity Attacks & Data Breaches and Leaks:**

Cybersecurity attacks, including phishing, ransomware, and malware, pose a constant risk to individuals and organizations. Attackers seek unauthorized access to sensitive data for financial gain or malicious purposes. Data breaches can lead to identity theft, financial fraud, and the exposure of personal information, causing significant harm to individuals or organization's reputation.

ii. **E-commerce and Digital Payments Risks:**

The growth of e-commerce and digital payments introduces risks such as payment fraud, unauthorized access to financial information, and breaches of online platforms. Individuals may experience financial loss, identity theft, and disruption of online transactions.

iii. **Data Localization Challenges:**

Data localization requirements may present challenges in ensuring secure storage and management of data within India, particularly for organizations with complex data processing operations. Compliance challenges may arise, and there could be an increased risk of unauthorized access to data during localization processes.

iv. **Lack of Awareness:**

Many individuals may lack awareness of digital privacy risks, safe online practices, and the importance of securing personal information. Inadequate awareness increases the likelihood of falling victim to cyber threats, phishing attacks, and other forms of digital manipulation.

v. **Emerging Technologies:**

The adoption of emerging technologies such as artificial intelligence (AI), machine learning, and blockchain introduces new privacy challenges, including algorithmic bias and data manipulation. Improper use of these technologies can exacerbate privacy risks, leading to discrimination and loss of control over personal information.

(E.) Balancing the Equation:

Navigating this complex landscape requires a multi-pronged approach that balances innovation with data protection. Here are some key strategies:

i. **Transparency and accountability:**
Organizations must be transparent about their data collection practices and accountable to citizens for its use. This includes clear privacy policies, robust oversight mechanisms, and accessible avenues for redress.

ii. **Privacy by design:**
Data protection principles should be embedded into the design of new technologies and processes, minimizing data collection and ensuring secure storage and access controls.

iii. **Empowering individuals:**
Citizens should have clear rights to access, control, and delete their personal data held by organizations. This includes the right to object to automated decision-making based on personal data.

iv. **Security by default:**
Robust cybersecurity measures should be implemented across all computerised

systems, with regular vulnerability assessments and penetration testing.

v. **Collaboration and knowledge sharing:**

Governments can learn from each other and collaborate with private sector experts to develop and implement effective data protection practices.

Implementing these strategies presents significant challenges. Governments often face resource constraints, complex legacy systems, and competing priorities. Striking a balance between security, efficiency, and user-friendliness can be difficult. However, several solutions are emerging:

a. **Privacy-enhancing technologies (PETs):** Tools like homomorphic encryption and secure multi-party computation allow data analysis without revealing individual information.
b. **Privacy-aware AI:** This field seeks to develop AI algorithms that are fair, unbiased, and respect individual privacy.
c. **Data minimization:** Collecting only the data necessary for a specific purpose and discarding it securely after use can significantly reduce privacy risks.
d. **Strong data governance frameworks:** Implementing clear policies and procedures for data management can ensure consistent and responsible data handling across Government agencies.

(F.) The DPDP Act, 2023: -

In early August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, 2023[6]. The DPDP Act is India's first data protection act, and it establishes a framework for the processing of personal data in India. The act applies to data collected online or offline, and later digitized.

(G.) Conclusion:

The evolving landscape of digital privacy in Indian Government organizations requires a nuanced and multifaceted approach. As India strides forward on the path of digital transformation, it is imperative to navigate the delicate balance between innovation and data protection. Government entities must not only comply with evolving regulatory frameworks but also foster an ethical and responsible approach to data usage. The journey toward balancing innovation and data protection is not a static one. It requires a dynamic,

adaptive, and collaborative effort from Government organizations, regulatory bodies, and citizens. In shaping a responsible digital future, India has the opportunity to set global standards for how technology can be harnessed for progress while respecting the fundamental right to privacy.

Suggested Reading: -

1. A total of 65,893 cases were registered under cybercrimes, showing an increase of 24.4% in registration over 2021 (52,974 cases).
2. Big tax fraud: How stolen identities were used to fake GST registration.
3. Jalandhar resident becomes a victim of identity theft-6 loans worth Rs 4 lakh taken in his name by a fraudster from three different banks & 3 finance companies.
4. The Exploitation of Personal Data in Hungary's 2022 Elections.
5. Your data and how it is used to gain your vote.
6. The Most Important Things to Know About Apps That Track Your Location.
7. Mobile Privacy: What Do Your Apps Know About You?

References:

1. https://thewire.in/law/supreme-court-aadhaar-right-to-privacy
2. https://www.vox.com/future-perfect/21420357/kenya-mobile-banking-unbanked-cellphone-money
3. https://www.linkedin.com/company/uk-biobank/?originalSubdomain=uk
4. https://www.bbc.com/news/world-us-canada-23123964
5. https://www.meity.gov.in/content/gi-cloud-meghraj
6. https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Act,_2023

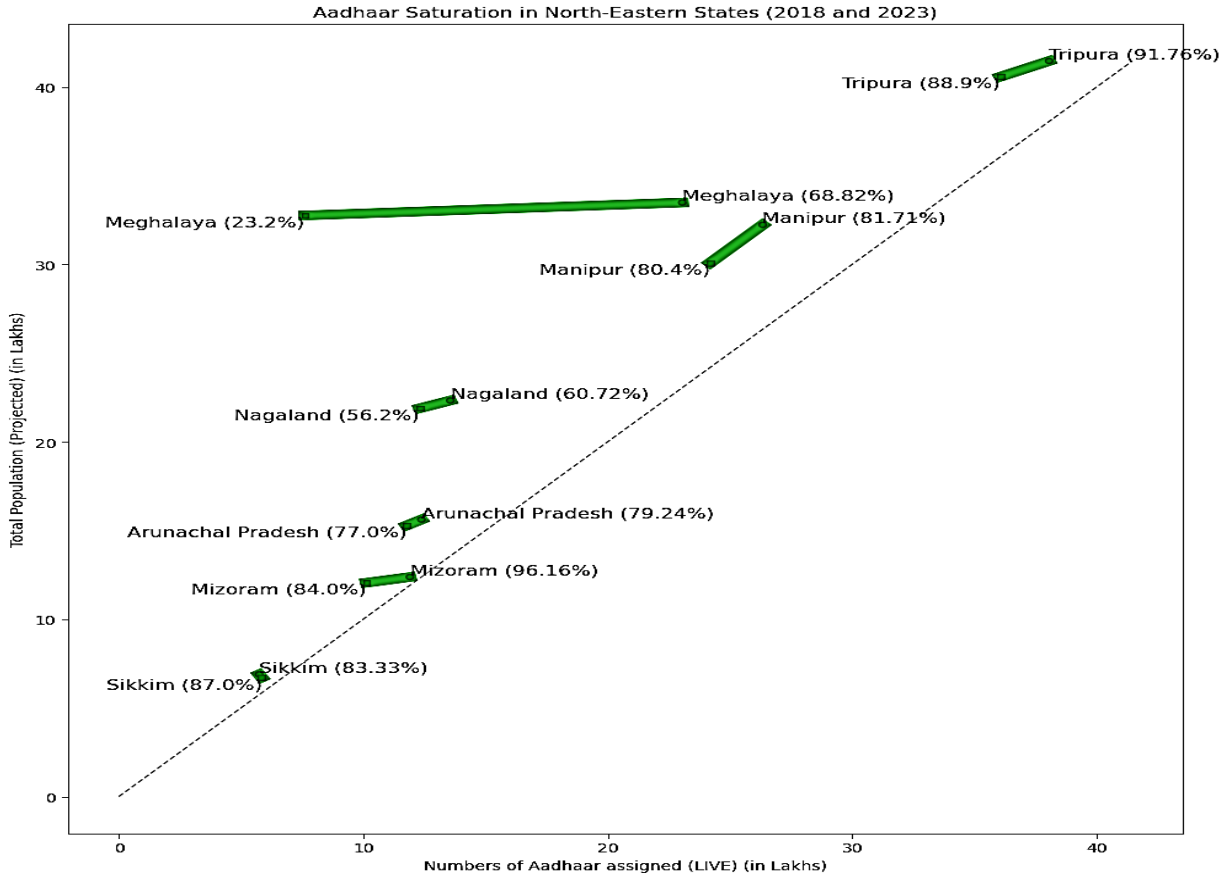
DATA PROTECTION AND PRIVACY- UTILITY TRADEOFF

By Sh. Rahul Kumar, Director (Training & Research), iCISA

Shri Rahul Kumar is 2015 batch IA&AS officer. He graduated in Mathematics & Computer Science from Chennai Mathematical Institute. Currently he is posted as Director (Training & Research) at iCISA, Noida.

The article examines the role of data-centric platforms in India's socio-economic development, focusing on initiatives like Aadhar, UPI, and DBT. It discusses the data lifecycle and privacy concerns, highlighting the risks of integrating databases and the limitations of traditional anonymization methods. The concept of differential privacy is presented as a robust solution for balancing data utility and individual privacy, emphasizing the importance of legal frameworks like the Digital Personal Data Protection Act, 2023.

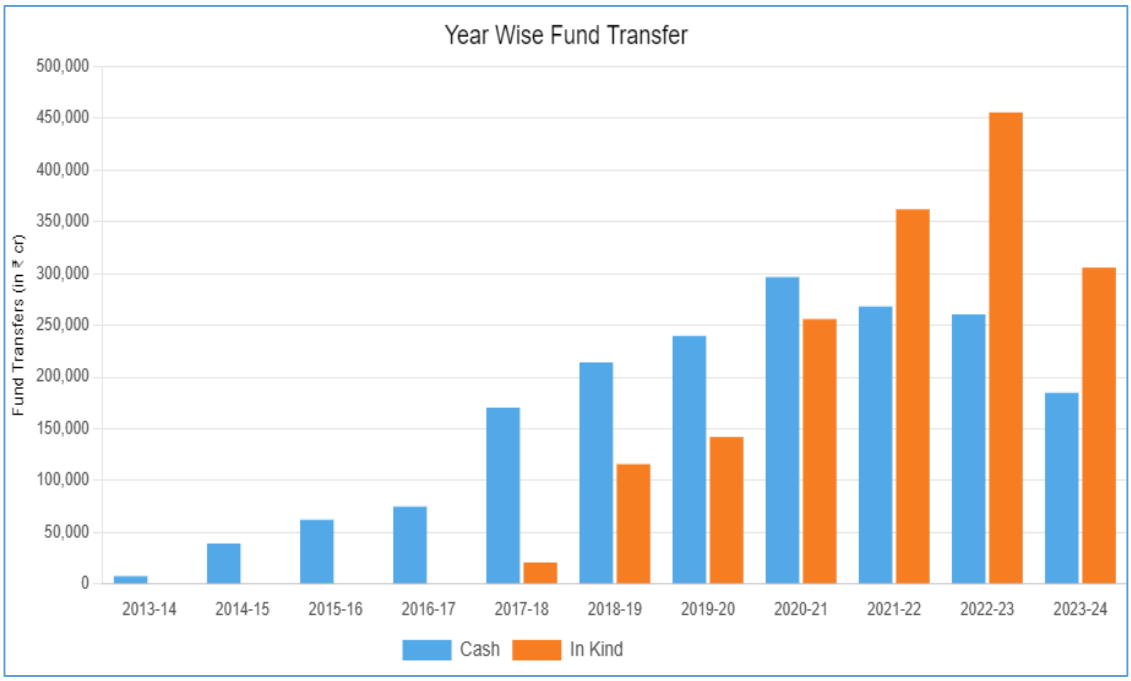
The trajectory of development and socio-economic empowerment in India increasingly hinges on data-centric platforms. These platforms, often rolled out on a population-wide scale, revolve around key pillars such as Aadhar for identity verification, UPI (Unified Payment Interface) and DBT (Direct Benefits Transfer), leveraging E Kuber for direct transfers, etc. This trend is also seen, in the charts below for some NER states where the coverage of Aadhar has increased significantly in last 5 years[1].



(The saturation ratio in brackets is arrived by dividing Aadhar Assigned with the Population.)

[1] Data from UIDAI 2018 and 2023, Chart self-generated. Assam not included as it skewed the chart due to large population.

Moreover, private entities across domains have widely embraced the India Stack platform, with its multifaceted technological infrastructure. Consequently, citizens navigate intricate data landscapes as they interact with these systems and leave trail of data. The data lifecycles—comprising acquisition, processing, analysis, visualization and storage —within these platforms and databases exhibit varying degrees of privacy and security safeguards.



(Union fund transfers to citizen over the decade)

While these data-driven platforms have ushered in unprecedented efficiency and accessibility, they also raise critical concerns regarding privacy and security safeguards. The lifecycles of personal data within these systems exhibit varying degrees of protection, necessitating a delicate balance between facilitating societal empowerment and upholding individual privacy rights.

Integration and Interpretation

There are now instances of governments, private sector entities using analytical methods, big data, machine learning and AI to gain insights from data. This is sometimes done by joining different datasets, and integrating various sources of data to uncover patterns, trends, and correlations that can provide valuable insights into stakeholders' behaviour, preferences, and needs. But any endeavour to integrate databases runs the risk of loss of privacy. The classical methods of data anonymization and pseudonymization for such circumstances, have now started to raise concerns of risk.

In a classical research on privacy conducted by Latanya Sweeney, a Harvard professor, in 1996 demonstrated the risk of data de-anonymization, demonstrating that an anonymized medical dataset that was in the public domain, can be used to identify individuals, regardless of the removal of all explicit identifiers, when the medical dataset was combined with a public voter list. (chart above) Sweeney found that 87% of the US population in a censorship dataset, could be identified by combining data attributes which are known as quasi[2]-identifiers[3].

This debate further led to privacy focused legislation in 1996 called HIPPA (Health Insurance Portability and Accountability Act) in USA.

To resolve this situation, the k- anonymity algorithm was introduced by Sweeney in 1998.

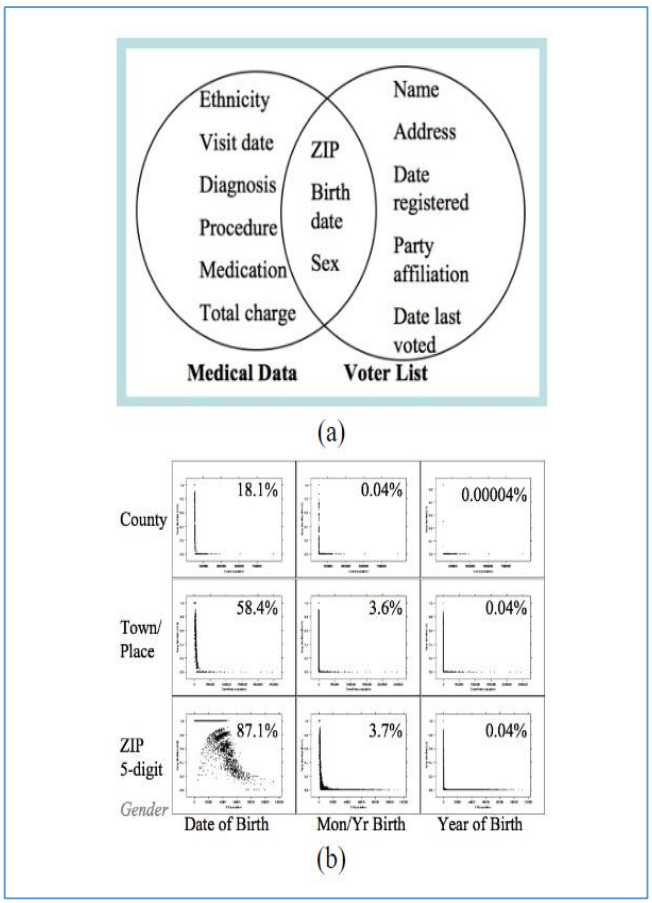


Chart above shows the ability to analyze and cross-reference demographic information from the combined medical and voter data sources, enabling the re-identification of individuals based on specific combinations of attributes. For eg: 87.1% of the population in the United States had characteristics that made them uniquely identifiable based only on three attributes of {5-digit ZIP, gender, date of birth}

[2] https://en.wikipedia.org/wiki/Latanya_Sweeney

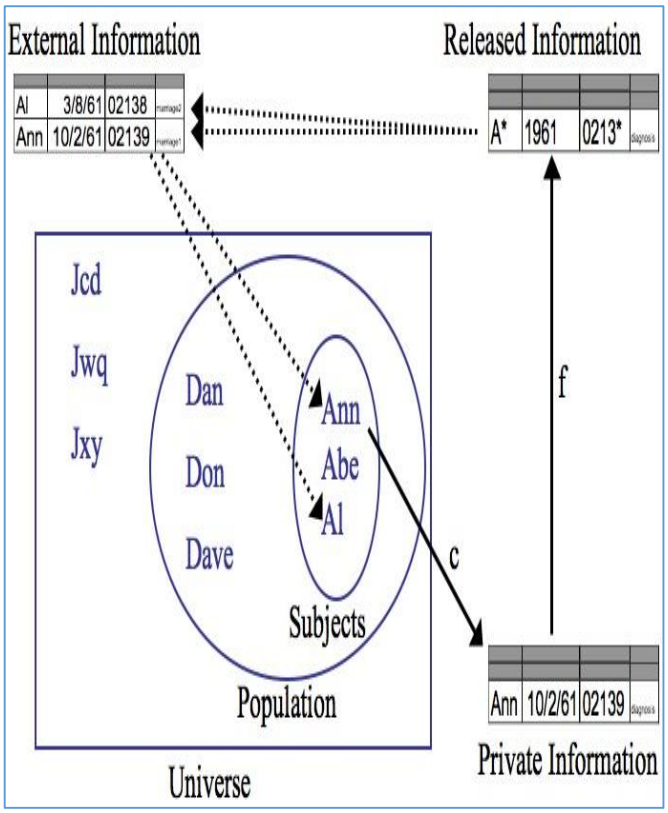
[3] https://latanyasweeney.org/work/identifiability.html https://dataprivacylab.org/projects/identifiability/paper1.pdf .

(The Explicit identifiers are those which can directly link to a person, like name, Aadhar etc. Indirect / Quasi identifiers are those which can indirectly but precisely identify a person when mixed with attributes like Zip, Birth Date etc)

In the chart on right[4], K-anonymity ensures that each record in a dataset is indistinguishable from at least (k-1) other records when certain identifying attributes are considered. The crucial theory behind k-anonymity is to ensure that for any attempted combination of quasi-identifiers (such as age, gender, zip code), there are at least k individuals who share that combination, thereby preventing unique identification. This makes it difficult to re-identify individuals based on the released data, as each record is same as at least (k-1) other records for those attributes.

This method of finding the optimal k anonymization for a dataset was considered, in technical terms as NP hard (ie, it cannot be cracked even with enormous computational resource)[5].

However, as it not randomized, therefore the concept of Differential privacy emerged for databases as a more robust approach to safeguarding privacy in data analysis. It adds noise to query responses, ensuring that the inclusion or exclusion of any individual's data doesn't significantly impact the outcome of the analysis. This approach has gained traction in both research and industry settings as a more effective means of balancing data utility with privacy protection. It is also more mathematically rigorous and gives a guaranteed privacy limit to the database.



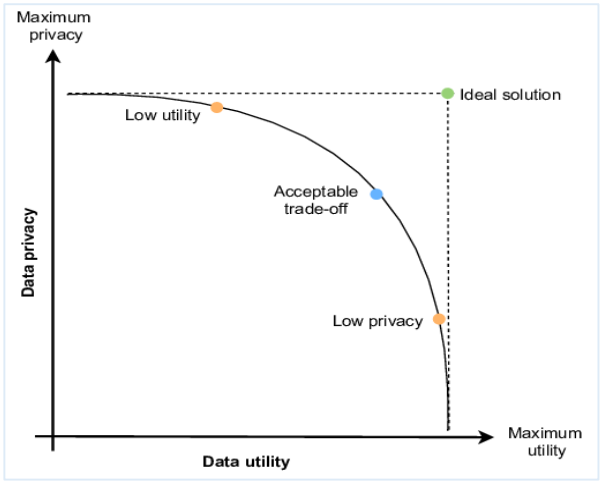
Here individuals (Ann, Al) have specific personal details like birth dates (3/8/61, 10/2/61) and zip codes (02138, 02139) as external information. To anonymize the data for release, the identifying details like dates are generalized to years (1961), and codes are suppressed to code (0213*) and name to (A*), such that each combination of attributes in the released information maps to at least k individuals. (Sweeney, 1998)

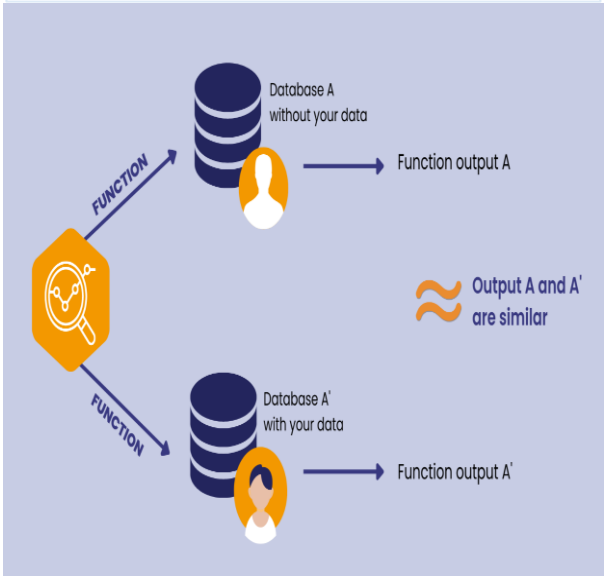
[4] https://latanyasweeney.org/work/kanonymity.html

[5] NP hard stands for Non-Deterministic Polynomial-time hard. These are problems for which finding a solution is extremely challenging and often infeasible within a reasonable timeframe. However, if you are given a solution, you can verify its correctness relatively quickly (in polynomial time).

Differential Privacy

It is an approach, devised in 2006, which provides a mathematical framework for providing privacy while sharing information about a group of individuals, by describing the patterns within the group while withholding information about specific individuals. This is done by making arbitrary small changes/ adding noise to individual data that do not change the statistics of interest. Thus, the data cannot be used to infer much about any individual[6]. This ensures that privacy is ensured even when the adversary knows the method of data collection and has unlimited computation.





> An algorithm is differentially private if an observer seeing its output cannot tell whether any particular individual's information was used in the computation. For eg: For a Function (seeking average pension) from PSAI pensioners' database if we have A(without a particular pensioners' data) and A'(with the full data), differential privacy ensures that the outputs from both are statistically indistinguishable despite A not having the original data.

Central to the differential privacy is the concept of Privacy Utility trade-off and the concept of ε (epsilon) Differential privacy. The Privacy-Utility Trade-off refers to the balancing act between preserving individual privacy and maintaining the usefulness or utility of the data for analysis and insights.

As seen here; if we prioritize privacy too much by adding a lot of noise, the data may become too distorted or inaccurate for

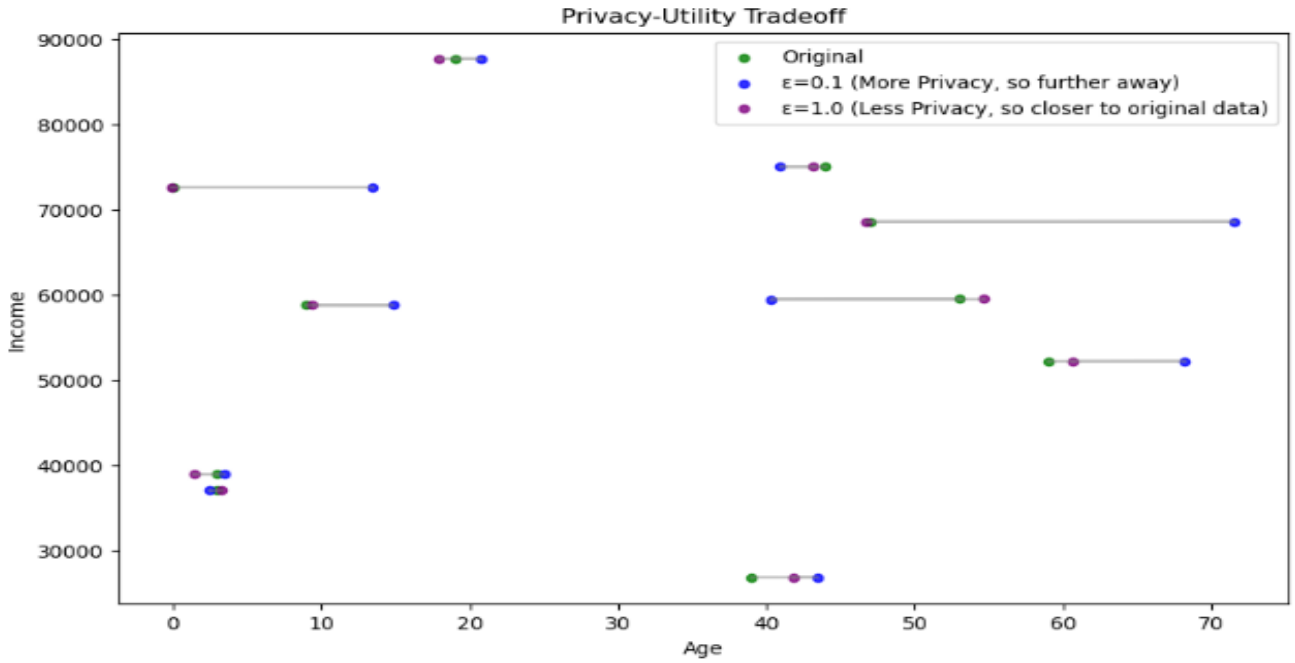
[6] Wikipedia definition; diagram, Trade-off chart, From https://www.statice.ai/post/what-is-differential-privacy-definition-mechanisms-examples

meaningful analysis. On the other hand, if we prioritize utility by adding little to no noise the risk of exposing individuals' private information is high.

The level of privacy protection provided by differential privacy is controlled by a parameter called epsilon (ε). A smaller value of ε means stronger privacy protection, but also less accurate results from queries on the data, thereby reducing the utility of the dataset. Similarly, a large ε, is less privacy enabling and thereby provides more flexibility of the usage of data for full analysis. The Laplace mechanism is a common way to achieve ε-differential privacy by adding noise drawn from a Laplace distribution to the query results.

Therefore, the goal is to find the right balance or trade-off between privacy and utility, ensuring that individuals' privacy is protected while still allowing for valuable insights and analysis to be derived from the data. This is even more important in current trend of Open data platforms which the governments all around the world, encourage.

In chart below[7] , on a dataset with age being a sensitive attribute (which has implications for privacy) the operation is performed to enable it to view clearly the output on one attribute of dataset showing impact on overall data.



Way ahead

The landmark judgment of Justice K.S. Puttaswamy vs Union of India, delivered on August 24, 2017, by the Supreme Court of India, recognized privacy as a fundamental right under the Constitution. It also emphasized the role of balance in data privacy and legitimate interests of the state.

[7] Random data by self, Chart self-Generated

It said "… requires a careful and sensitive balance between individual interests and legitimate concerns of the State. The legitimate aims of the State would include for instance protecting national security, preventing, and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union Government while designing a carefully structured regime for the protection of the data…."

The crucial role of such balance, can be enabled by the data protection frameworks of both privacy and security. This is done by legal frameworks (like Digital Personal Data Protection Act 2023) as well as adherence to new privacy embedded architectures (like CoWin, Aadhar etc) and privacy enabling algorithms (like differential privacy, k anonymity, l-diversity etc as discussed above). This would also free up the various datasets with governments and private entities for enhanced analysis and getting better socio-economic insights. These possibilities can be seen in:

- Analysis of Census Data for demographic trends by govt and civil society. Census data is already released by using differential privacy-based frameworks.
- Use differentially privacy-based techniques to analyze mobility data from various sources to improve urban planning and transportation systems without compromising individual privacy.
- using differential privacy to anonymize and share sensitive healthcare data for research purposes while adhering to the data privacy requirements outlined in regulations like the DPDP Act.
- governments can explore opportunities to monetize or share aggregated, anonymized data with private entities for research and development purposes
- governments can release differentially private transportation data to private companies developing smart city solutions, enabling innovation while protecting citizen privacy.

Data is said to be the new oil and will fuel the future engines of growth and innovation. It is in that context that an understanding of the data landscape, with the availability of legal and technical tools, will enable the maximizing of the overall social benefits without compromising the privacy

Government Initiatives for Digital Inclusion and Data Protection in India

By Sh. Sameer Asif, AAO/AMG-III, O/o DGA (I&CA), New Delhi

Mr. Sameer Asif is currently working as Assistant Audit Officer in AMG-III section of O/o DGA ICA New Delhi since September 2022.

This article discusses India's digital transformation, emphasizing the intertwined goals of digital inclusion and data protection. It highlights government initiatives like Digital India and PMGDISHA, aimed at improving access to technology and digital literacy for marginalized communities. Despite advancements, challenges such as regional disparities and rising cybercrime persist. The article also addresses legislative efforts, including the Personal Data Protection Act, 2023, and the establishment of regulatory bodies to ensure privacy.

Introduction

In contemporary India, technological advancements have ushered in an era of significant digital transformation. This shift impacts various aspects of life, including economic development, governance, social inclusion, and individual empowerment. At the core of this transformation are two intertwined imperatives: digital inclusion and data protection.

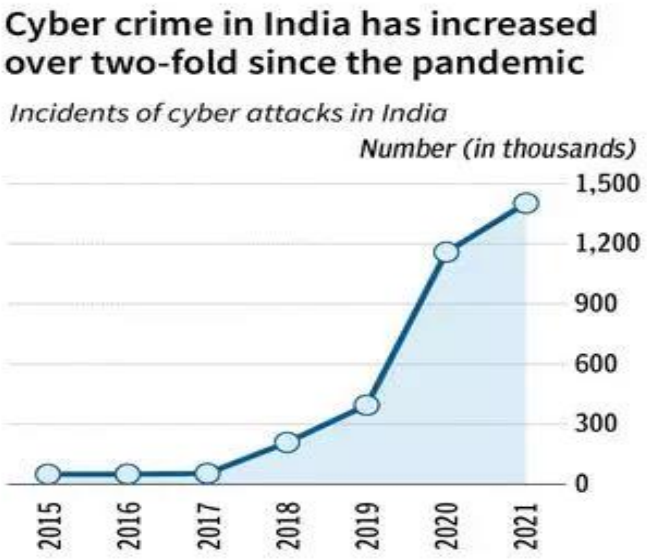


Image source 1: The Hindu Business Line

Digital inclusion, ensuring equitable access to digital technologies for social and economic progress, is central to India's vision for inclusive growth. Government initiatives focus on expanding digital infrastructure, promoting literacy, and empowering marginalized communities.

The rise in cybercrimes poses a significant challenge globally and in India. With increasing reliance on digital technologies, cybercriminals exploit vulnerabilities for financial gain and data theft. Collaborative efforts among governments, law enforcement, and cybersecurity experts are crucial to address these threats. Strengthening cybersecurity frameworks and promoting awareness are essential to mitigate risks and safeguard digital ecosystems.

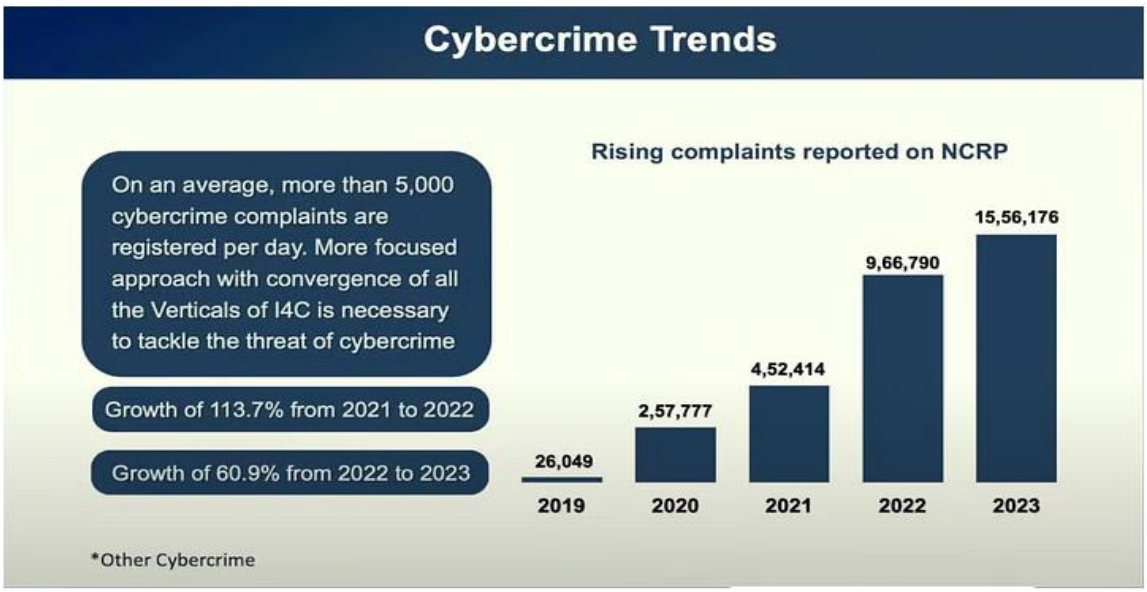


Image source 2: Scroll

Simultaneously, the expanding digital footprint raises concerns about data privacy, security, and sovereignty. With the widespread collection and processing of personal data, questions arise about individual rights, regulatory frameworks, and data protection mechanisms. In response, the government has taken significant steps, formulating policies, enacting legislation, and establishing regulatory bodies. These efforts aim to create a robust legal framework balancing innovation, economic growth, and individual privacy.

Evolution of Digital Initiatives in India

India's digital transformation journey has been shaped by strategic policy frameworks, legislative measures, and technological innovations. The Information Technology Act, 2000 (IT Act 2000) marked the country's first steps into the digital age, providing legal recognition for electronic transactions, signatures, and governance. This legislation facilitated e-commerce growth, addressed cybercrimes, and built trust in online transactions.

Building on the IT Act 2000, India pursued digital empowerment and inclusive growth. Initiatives like the National e-Governance Plan (NeGP) and State Wide Area Network (SWAN) aimed to bridge the digital divide by providing citizens access to government services digitally. Digital India, launched in 2015, aimed to transform India into a digitally empowered society and knowledge economy. Flagship programs like BharatNet and Common Service Centres (CSCs)

democratize access to services, particularly in rural areas.

India prioritized protecting digital assets and citizen privacy, evident in the Personal Data Protection Act, 2023. This legislation regulates personal data processing, fostering trust and accountability in the digital ecosystem. India's digital landscape thrives with a vibrant startup ecosystem, supported by initiatives like Startup India and the Atal Innovation Mission, driving innovation and entrepreneurship globally.

Current Landscape of Digital Inclusion/ Disparities

The current landscape of digital inclusion in India presents a multifaceted scenario marked by advancements alongside persistent challenges. At the forefront of this landscape are considerations of access to technology, internet penetration rates, and levels of digital literacy, which collectively shape individuals' engagement with the digital ecosystem across the nation.

Access to Technology and Internet Penetration: Access to technology remains a critical determinant of digital inclusion, influencing individuals' ability to engage with digital platforms and services. While urban areas boast relatively high levels of technological access and internet connectivity, rural and remote regions continue to face challenges due to infrastructural limitations and connectivity gaps. Initiatives like the BharatNet project aim to bridge these disparities by providing broadband connectivity to gram panchayats. However, despite efforts to expand digital infrastructure, disparities persist, hindering the equitable distribution of digital resources.

Disparities in Digital Literacy: Variations in digital literacy levels further exacerbate disparities in digital inclusion. While certain segments of the population demonstrate proficiency in basic digital skills, a significant portion lacks the necessary knowledge and competencies to navigate digital platforms effectively. These disparities are particularly pronounced across demographic lines, with factors such as age, gender, education level, and socio-economic status influencing individuals' digital literacy levels and access to digital resources.

Regional Disparities: Regional differences play a significant role in shaping digital inclusion outcomes, with variations observed between states and geographical regions. Southern and western states tend to exhibit higher levels of digital literacy and internet penetration compared to their northern and eastern counterparts. These regional discrepancies are influenced by

factors such as economic development, infrastructure availability, and government interventions, highlighting the need for targeted strategies to address disparities at the regional level.

Demographic Factors: Demographic factors also contribute to disparities in digital inclusion, with age, gender, education level, and socio-economic status serving as key determinants of individuals' digital literacy levels and access to digital resources. Marginalized communities, including women, rural populations, and individuals with lower levels of education and income, often face heightened barriers to digital inclusion, exacerbating existing disparities and hindering socio-economic advancement.

Addressing these disparities requires comprehensive strategies that prioritize equitable access to technology, localized interventions, and efforts to enhance digital literacy across diverse demographics. By bridging these gaps, India can work towards creating a more inclusive digital ecosystem that benefits all segments of society.

Government's Role in Strengthening Data Protection

The Indian government plays a pivotal role in fortifying data protection measures, employing a multifaceted approach to navigate the complexities of the digital landscape. Key legislations such as the Personal Data Protection Act 2023 and the proposed Digital India Act 2023 establish a robust legal framework, regulating data collection, processing, and storage. These laws safeguard individuals' privacy rights and foster responsible data management practices across businesses and government entities.

Supplementing legislative efforts, regulatory bodies like the Data Protection Authority (DPA) ensure effective enforcement of data protection laws. The DPA oversees compliance, issues guidelines, and adjudicates disputes concerning data protection violations. Additionally, collaboration between the Ministry of Electronics and Information Technology (MeitY) and sectoral regulators ensures consistent enforcement across various sectors, enhancing regulatory efficacy.

Through these initiatives, the government aims to cultivate trust and confidence in India's digital ecosystem while stimulating innovation and economic growth. By prioritizing data protection and privacy, the government demonstrates its commitment to upholding fundamental rights in the digital age and fostering a secure and inclusive digital environment for all citizens.

Government Policies and Programs for Digital Inclusion

Government-led initiatives play a pivotal role in driving digital inclusion efforts in India, with a focus on bridging the digital divide and empowering citizens through technology.

Digital India Initiative

At the forefront of India's digital inclusion agenda is the Digital India initiative, launched in 2015 with the vision of transforming the nation into a digitally empowered society and knowledge economy. This comprehensive program encompasses various flagship initiatives aimed at expanding digital infrastructure, promoting digital literacy, and enhancing the delivery of digital services to citizens across the country.

Digital India aims to bridge the digital divide by leveraging technology to empower citizens, particularly those in rural and remote areas. Through initiatives such as BharatNet, which seeks to provide broadband connectivity to gram panchayats, Digital India aims to democratize access to digital resources and enable last-mile delivery of government services. Additionally, the initiative focuses on promoting digital literacy and digital skills training through programs like Digital Saksharta Abhiyan and National Digital Literacy Mission, thereby equipping citizens with the necessary knowledge and competencies to participate in the digital economy.

Image source 3: National Informatics Centre

Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)

PMGDISHA, launched in 2017, is a flagship program under the Digital India initiative aimed at making six crore persons in rural areas digitally literate, reaching to around 40 % of the rural households by covering one member from every eligible household. Through a network of training centers and awareness campaigns, PMGDISHA seeks to impart basic digital skills to rural populations, enabling them to leverage digital technologies for socio-economic development. The program focuses on empowering individuals with essential digital literacy skills, including operating digital devices, accessing digital services, and engaging in digital transactions.

The Cyber Surakshit Bharat (Cyber Safe India) Program-

An initiative launched by the Government of India aimed at enhancing cybersecurity awareness and capacity across the nation. Introduced under the aegis of the Ministry of Electronics and Information Technology (MeitY), in collaboration with the National e-Governance Division (NeGD) and industry partners, the program seeks to create a safer digital ecosystem for citizens, businesses, and government entities.

In response to these challenges, the Indian government has implemented various initiatives aimed at promoting digital inclusion and bridging the digital divide. Programs such as Digital India, Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA), Cyber Surakshit Bharat Pragramme and BharatNet are designed to provide digital infrastructure, training, and support to underserved communities, with a focus on empowering rural populations and marginalized groups.

Other Schemes Fostering Digital Literacy and Access

The Indian government has implemented schemes like the Common Service Centres (CSCs) under the National e-Governance Plan (NeGP) since 2006, providing digital services in rural areas. Collaborations with private sector and civil society have enriched initiatives like Digital Saksharta Abhiyan for marginalized communities and partnerships with telecom for affordable internet access. Challenges persist, including infrastructural limitations and socio-cultural barriers. Yet, mobile technology, digital payments, and localized content present opportunities to enhance digital inclusion and reach underserved populations.

Data Protection Laws and Regulations in India

India's data protection framework has undergone significant evolution in recent years, with the enactment of key legislations and regulations aimed at safeguarding individuals' personal data and ensuring privacy in the digital age.

1. Information Technology Act 2000 (IT Act 2000)

The IT Act 2000 serves as the foundational legislation governing electronic transactions, digital signatures, and cybercrimes in India. Enacted to provide legal recognition for electronic records and facilitate e-commerce activities, the IT Act 2000 laid the groundwork for addressing cybersecurity concerns and protecting digital assets. While the IT Act 2000 established the legal framework for digital transactions and cybersecurity, the absence of comprehensive provisions for data protection necessitated further legislative measures.

2. Personal Data Protection Act 2023

Derived from the Digital Personal Data Protection Bill introduced in 2019, the Digital Personal Data Protection Act 2023 represents a significant milestone in India's data protection landscape. The Act aims to regulate the processing of personal data and safeguard individuals' privacy rights in the digital realm. It establishes principles for the collection, storage, processing, and transfer of personal data, empowering individuals with rights such as the right to access, rectification, and erasure of their personal data. The Act also mandates the establishment of a Data Protection Authority (DPA) tasked with enforcing data protection laws, regulating data processors and controllers, and adjudicating disputes related to data protection violations.

3. Proposed Digital India Act 2023

The proposed Digital India Act 2023 provides a broader legal framework for digital governance, cybersecurity, and data protection. Encompassing provisions related to data localization, cross-border data transfer, and cybersecurity measures, the Act seeks to strengthen India's digital infrastructure and promote trust in the digital ecosystem. By addressing critical issues such as data sovereignty and cybersecurity threats, the proposed Digital India Act 2023 complements the Personal Data Protection Act 2023, reinforcing India's commitment to safeguarding digital assets and promoting responsible data management practices.

Legal Landscape and Regulatory Bodies

The legal landscape governing data protection in India is characterized by a multi-faceted approach involving legislative enactments, regulatory bodies, and judicial pronouncements. Key regulatory bodies responsible for overseeing data protection and privacy include:

Data Protection Authority (DPA): Established under the Digital Personal Data Protection Act 2023, the DPA serves as the primary regulatory authority responsible for enforcing data protection laws, regulating data processors and controllers, and adjudicating disputes related to data protection violations.

Ministry of Electronics and Information Technology (MeitY): MeitY plays a pivotal role in formulating policies and regulations related to data protection, overseeing the implementation of the IT Act 2000, and promoting cybersecurity initiatives across various sectors.

Sectoral Regulators: Certain sectors, such as telecommunications and banking, have their own regulatory authorities (e.g., Telecom Regulatory Authority of India, Reserve Bank of India) responsible for ensuring compliance with data protection norms specific to their respective industries.

Judiciary: The Indian judiciary, through its interpretation of constitutional provisions and statutory laws, plays a crucial role in adjudicating data protection cases and setting legal precedents that shape the evolving landscape of data protection jurisprudence.

CYBER SECURITY HIERARCHY IN INDIA

PM OFFICE/ CABINET SECY (PMO/ CAB SEC)	MINISTRY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANISATION (NGO)
NATIONAL SECURITY COUNCIL (NSC)	NATIONAL CYBER COORD CENTRE (NCCC)	AMBASSADORS & MINISTERS	TRI SERVICE CYBER COMMAND	DEPARTMENT OF INFORMATION TECHNOLOGY (DIT)	CYBER SECURITY AND ANTI HACKING ORGANISATION (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre(NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development In India (CECSRDI)
Joint Intelligence Group (JIG)	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Education Research Network (ERNET)	Cyber Security of India(CSI)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center (MAC)			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

International Comparisons and Best Practices

India can strengthen its government initiatives for digital inclusion and data protection by analyzing similar programs worldwide. Comparative studies offer insights for policymakers navigating digital governance complexities. By learning from leading policies, countries can adapt innovative strategies to enhance their own data protection frameworks. This fosters dialogue, encouraging policymakers to assess practices critically and adapt strategies to unique contexts. Embracing continuous learning promotes innovation and collaboration, advancing the collective goal of building trust and safeguarding privacy in the digital era.

Key policies include:

General Data Protection Regulation (GDPR) - EU (2018): Grants individuals' control over personal data, harmonizing data protection laws.

Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada (2000): Regulates personal data handling by private sector organizations, ensuring transparency.

Act on the Protection of Personal Information (APPI) - Japan (2003): Governs personal information handling, emphasizing rights protection and accountability.

Privacy Act - Australia (1988): Governs personal data handling, promoting transparency and trust in digital practices.

Brazilian General Data Protection Law (LGPD) - Brazil (2020): Modernizes data protection, regulating data processing for transparency and accountability.

California Consumer Privacy Act (CCPA) - US (California) (2020): Grants robust data privacy rights to enhance consumer protection.

Personal Data Protection Act (PDPA) - Singapore (2012): Establishes rules for responsible data practices, upholding privacy rights.

Digital Identity Program- Denmark (2016)- Provides secure access to digital services, enhancing data protection through robust authentication and authorization mechanisms.

Challenges and Possible hurdles in India's Digital Road Ahead

Implementation Challenges:

Implementing digital inclusion and data protection initiatives faces hurdles such as resource constraints and bureaucratic inefficiencies. Streamlining processes and allocating adequate resources are essential to overcome these challenges and ensure effective program delivery.

Enforcement Hurdles:

Enforcing data protection laws poses challenges in monitoring compliance and addressing violations. Strengthening enforcement mechanisms, providing regulatory bodies with necessary resources and authority, and fostering collaboration with stakeholders can enhance enforcement effectiveness.

Privacy Protection Measures:

Privacy concerns underline the importance of robust data protection measures. Enhancing data security, implementing stringent privacy policies, and raising awareness among citizens can address privacy concerns and strengthen trust in digital platforms.

Transparency and Engagement:

Enhancing transparency and stakeholder engagement is key to addressing critiques of government initiatives. By promoting transparency in decision-making processes and actively involving stakeholders in policy development, the government can build trust and foster collaboration in advancing digital inclusion and data protection.

Future Directions and Recommendations

As India advances towards digital inclusion and robust data protection, there are opportunities to enhance government initiatives and address challenges:

Integrated Approach: Combine digital inclusion and data protection efforts.

Targeted Interventions: Tailor programs for marginalized communities and rural populations.

Capacity Building: Invest in digital literacy to empower individuals.

Public-Private Partnerships: Collaborate to leverage resources and expertise.

Policy Coherence: Ensure alignment between policies.

Regular Evaluation: Assess progress and inform decision-making.

Enforcement Strengthening: Enhance regulatory oversight for compliance.

Adaptive Regulations: Develop flexible frameworks to address evolving risks.

Community Engagement: Involve grassroots organizations for relevance.

User-Centric Approach: Prioritize individual needs in service design.

Transparency and Accountability: Promote openness and feedback mechanisms.

Conclusion

In conclusion, as India accelerates its digital transformation journey, it is imperative for the government to reaffirm its commitment to digital inclusion and robust data protection. This call to action necessitates sustained efforts and collaboration across government agencies, private sector stakeholders, civil society organizations, and citizens. By prioritizing digital literacy, strengthening enforcement mechanisms, fostering public-private partnerships, and engaging communities in co-designing and implementing initiatives, India can ensure that its digital ecosystem is inclusive, secure, and empowering for all. Continued government commitment and collaboration are essential to realize the full potential of digital technologies in driving socio-economic development, while safeguarding individuals' privacy rights and enhancing trust in the digital environment. Together, let us work towards building a digitally inclusive and resilient India that leaves no one behind, setting a global standard for inclusive digital governance.

Suggested Reading:

1- "Data Protection: A Practical Guide to UK and EU Law" by Peter Carey
2- "Privacy Law Fundamentals" by Daniel J. Solove and Paul M. Schwartz
3- "The Personal Data Protection Bill, 2019: A Critical Appraisal" edited by Rahul Matthan and Anirudh Burman
4- "Cybersecurity in India: A Framework for National Security" by Balsing Rajput
5- "The IT Act and Digital Policy: A Citizen's Guide to Digital Law and Rights in India" by Rohini Lakshané and Vanya Rakesh
6- Information Technology (Amendment) Act, 2008
7- Personal Data Protection Act, 2023

Digital Data Protection: Role of SAI

By Sh. R. Jayaprakash

Mr. R Jayprakash is a retired Senior Audit Officer, experienced in audit of revenue, expenditure, public projects and Information Technology. He has also authored a book titled 'Handbook on Audit in PSU ERP' for Office of the DG of Audit (Finance & Communication), Delhi.

The article examines the significance of digital data protection amid the rapid growth of data in the digital age, emphasizing the distinction between data protection and privacy. It discusses the responsibilities outlined in the Digital Personal Data Protection Act, 2023, and highlights the role of the Supreme Audit Institution in ensuring data security and compliance. The authors stress the need for robust measures to prevent data breaches and enhance organizational accountability.

In a data driven world, digital data assumes significance as a valuable asset for all organizations. Safeguarding of these assets against leakage and misuse has become a management priority. Leakage of sensitive organizational data on management strategies, investment plans, product development etc. can adversely affect the business prospects. Safeguarding the digital data against loss, leakage, damage or corruption is a data protection issue. Another issue is that of data privacy, which is the right of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. Data protection is an organizational matter, whereas data privacy is a primarily a personal matter. The leakage of personal data has serious consequences of inviting penal action from regulatory bodies and legal claims on damages from the persons on breach of privacy. Since organizations collect, collates and control personal data of their customers, data privacy becomes part of the overall data protection strategy of the organizations.

Regulations on Data Protection and Data Privacy

The 4th Revolution (4R) in Information Technology has resulted in exponential growth of data. Government agencies also collect, collate and control tons of data on migration to IT systems and launching of e-governance initiatives. The general public also generates terabits of data from our routine activities, knowingly and unknowingly from use of mobile phones, internet and various other online activities. In 2010, the global data size was 2 Zettabytes, which grew in size to 79 Zb in 2023 and it is estimated to reach 181 Zb by 2025.

This exponential growth of data and its custody and control by multiple agencies in private and public sector has posed major threats on their leaks and consequent breach of privacy. The Information Technology Act 2000 (IT Act 2000) and rules made under it- the Information Technology Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SDPI Rules) provide for reasonable security practices and

procedures to be followed in protection of data including personal data.

But these rules were applicable only to entities engaged in commercial or professional sectors and not applicable to government on non-business entities.

The right to privacy was recognized as a fundamental right protected under Article 21 of [art III of the Indian Constitution by the Supreme Court in 2017 (Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.). This land mark judgment invoked efforts to formulate comprehensive legislation on protection of personal data, which culminated in enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act 2023).

Responsibilities and Rights Under The DPDP Act 2024

The Act defines personal data as any information that can directly or indirectly identify an individual. It applies to processing of personal data within India in digital format and non-digital data which is digitised subsequently. The Act also applies to such processing outside India, if it is for offering goods or services in India. The Act specifies the obligations of *Data Fiduciaries* (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data) and the rights and duties of *Data Principals* (that is, the person to whom the data relates). The Government has the right to designate certain Data Fiduciaries as *Significant Data Fiduciaries* (SDFs) on the basis of the volume and sensitive nature of personal data, broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The SDFs are required to appoint Data auditor and conduct periodic audit on the protection of personal data in the organization.

The primary responsibility of protection of personal data rests with the Data Fiduciary. Data Fiduciary can only process the personal data of a Data Principal for lawful purposes, with consent or for certain legitimate uses. The Data Fiduciary can appoint a Data Processor for processing the data, under a valid contract. The Data Fiduciary is also responsible to maintain accuracy and security of the data and to delete the data on the request of the Data Principal or once the purpose of holding the data has been met.

The Act provides for setting up of a Data Protection Board, which has the responsibility to adjudicate on non-compliance with the provisions of the Act. The Board enjoys the same powers as are vested in a civil court" – including summoning any person, receiving evidence, and inspecting any documents (Section

28(7)). The Board's orders are binding on the parties concerned. Affected parties can appeal against the decision of the Board before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

Role of Supreme Audit Institution in Protection of Personal Data

The Digital Personal Data Protection Act 2023 does not directly assign any role to the Supreme Audit Institution (SAI) in protection of personal data. But the SAI, by virtue of his constitutional mandate, has two distinct roles on protection of personal data. The first one is to give an assurance on the data security in the audited entities. The second one is to ensure data security within SAI.

1. **Assurance on Data Security in Audited Entities**

In compliance with the provisions of the DPDP Act 2023, SAI India has notified the "Policy on Data Governance and Data Security" in July 2024. The policy objectives include (i) ensuring compliance with the statutory framework of Government of India related to data governance and security (ii) providing framework for management of diverse types of data utilized in the IA&AD and ensure its security and (iii) addressing the concerns related to privacy of individuals and utilization of data held in fiduciary capacity in the Department. As per the policy, an officer at DG/PD level, designated as the Chief Information Security Officer (CISO) in IS wing at the office of C&AG of India shall be responsible for supervising the overall security landscape of the organization, defining security standards and implementing latest security solutions and technologies. The Heads of the Wings at HQ Office and the HoDs of the field Offices designated as Data Owners have the authority to make decisions about data access, usage, and retention within their jurisdiction. The Data Owners in field offices will nominate a Data Protection Officer (DPO), who shall be responsible for management of data in each of the Field Offices. The DG/PD (IS Wing) is designated as the Chief Data Protection Officer (CDPO) for data governance and as the Chief Information Security Officer (CISO) for the Department, as per the Guidelines issued by the Indian Computer Emergency Response Team (CERT-IN).

2. **Assurance on Data Security Within SAI**

While auditing, the team has the right to access the data maintained by the audited entity in fiduciary capacity. Audit's access includes "all data, information and documents, including electronic data and access to information systems of the auditable entity, as may be required and asked for by Audit. Audit's access includes complete and timely access to

confidential and sensitive data, information or documents, handling of which will be governed by Regulation 20." *(Regulations on Audit & Accounts 2020, Ch 4.1).*

The nature of citizens' data included data on income, social security, health, census, employment, crime etc which are collated and analyzed by CAG auditors using data analytic tools. The audit team holds these data in a fiduciary capacity and the Guidelines on Data Analytics 2017 underlines the importance of maintaining security of such data. The Guidelines include, (i) safe custody of all data (2) confidentiality of data (3) limit on the number of persons who can access the raw data (4) unauthorized disclosure by auditors etc. *(Guidelines on Data Analytics 2017, Para 2.15 -2.18).*

The auditors have the obligation to maintain confidentiality of information and protection of personally identifiable/sensitive information acquired during audit *(Regulation 20).* If certain privileged or confidential information or Personally Identifiable Information (PII) prohibited from general disclosure by law is obtained in course of an audit, then the Auditors are required to maintain confidentiality of that information and ensure that any audit products do not become a means of compromising such privilege or confidentiality of the information *(Regulation 20(2)).*

The OIOS (One IAAD One System), the audit platform by SAI makes access and collection of entity data easy. There needs to be sufficient controls on the nature of data accessed by audit and custody of data. Adequate information security systems are crucial in the OIOS to safeguard against unauthorized access, corruption and data loss. SAI is giving due care and diligence on the security issues connected with OIOS.

"SAI India is working towards formulating data policy, governance principles, access protocols and security policy to give assurance to auditee for data safety and legitimate use. The role of auditors is going to be critical in such a context since AI is still a little understood technology, mostly opaque in its operations and needs to be evaluated in terms of ethics and responsibility." *(OIOS Press Release CAG 31/3/2023).*

Conclusion

The audits facilitate by assessing the IT systems which safeguard the digital data security in the audited entities through performing necessary data security related checks and reporting the deficiencies to the management for corrective action.

Deciphering the DPDP Act: A Critical Exploration of its Core Principles, Strengths, and Constraints from the Perspective of Digital Natives of India

By Dr. Charru Malhotra[8] and Sh. Udbhav Malhotra[9]

ABSTRACT

The swift expansion of platform-based services has led to an intensive collection, preservation, and examination of data by numerous service providers. This accumulation of extensive personal data reservoirs is not only exploited for monetary gain by these providers but also poses a risk of unauthorized access and clandestine misuse by malicious entities. Moreover, the resurgence of Artificial Intelligence (AI) technology has intensified concerns regarding the privacy of individuals. India, as a national commitment to enhance the 'Ease of Living' for its digital natives, passed its Digital Personal Data Protection (DPDP) Act on August 11, 2023. The authors attempt to explore the DPDP Act of India for its key tenets, strengths, and

The article critically examines India's Digital Personal Data Protection (DPDP) Act, enacted in August 2023, amidst growing concerns over data privacy and misuse in the digital age. It outlines the Act's core principles, strengths, and limitations, emphasizing its potential to protect digital natives while highlighting areas for improvement, such as enhancing consent mechanisms and the authority of the Data Protection Board. The authors advocate for a more robust regulatory framework to adapt to rapid technological changes and better safeguard individual privacy rights.

[8] Prof. (Dr.) Malhotra has more than thirty-three years of experience in the digital domain with core areas of expertise in 'Public Policy Formulation for Digital Technologies', 'AI and Ethics', 'Design Thinking' 'Digital Transformation in Governance', Smart Cities', and 'Cyber Security'. As one of the seniormost professors at the Indian Institute of Public Administration (IIPA) and as the Lead Coordinator (Centre of e-Governance and ICT) at IIPA, she is currently involved in the capacity building of senior government officers and research consultancy and advisory practices related to digitalization and future of organizations. Several global and national agencies have sought her expertise for curating new digital propositions and better technology policy space including the Government of India's (GoI) "Sectoral Group of Secretaries (SGOS-9) on Governance" that was comprised 10 ministries and departments of GoI for preparing the vision of ***Viksit Bharat* @2047.** She is a doctorate from IIT-Delhi.

[9] Udbhav Malhotra is currently engaged as an Intern at NitiAyog in the Education domain where he is working on several aspects of the New Education Policy (NEP, 2020). Before, for more than a year, he served as a short-term intern at the Indian Institute of Public Administration (IIPA) in New Delhi, focusing on public policy analysis with a specialization in artificial intelligence, data governance, and cyber security. In both these roles, he supports the study and SWOT analysis of tech-policy regulations, undertakes literature reviews, and assists in preparing materials for policy deliberations and workshops. He has contributed to several publications related to AI, cyber security, and data protection laws.

limitations. To do so, literature has been reviewed to understand the basic principles of privacy and data protection with special reference to the DPDP Act and some of its previous avatars. This desktop research armed the authors to undertake a critical analysis of the DPDP Act with specific recommendations from the perspective of its digital natives. The study affirms that the Digital Personal Data Protection (DPDP) Act of 2023 is a step in the right direction and there are some potential areas for improvement, such as addressing the nuances of consent and data principal awareness. The study further laments that the scope and authority of the envisioned Data Protection Board (DPB) body are insufficient for proactive enforcement in a country like India. Therefore, the authors suggest a need for a more robust framework to ensure compliance and protect the rights of digital natives. Since there is a global trend towards stronger data protection laws than DPDP and more particularly respecting the diverse profile of digital natives in India, authors suggest that in the forthcoming DPDP rules 'Exceptions' must be carefully tailored to delicately balance individual privacy rights with national innovation spirit and security needs.

Keywords: Privacy, Data Protection, Data Fiduciary, Data Principal, Data Protection Board, DPDP Act, India Stack, Digital India, Artificial Intelligence (AI), Data breach, Digital natives, New Age Technologies (NATs), Digital Transformation of Public Sector, India, Cyber security, Personal data, Techno-legal legislations, Public Policy.

SECTION 1: INTRODUCTION

The renewed use of Artificial Intelligence (AI) has shaped individual privacy concerns. There is a relentless gathering, storage, and analysis of data by various kinds of service providers. These vast data lakes of personal data, not only get monetized by the service providers but could also be stolen and stealthily misused by other rogue actors. The recent data breaches at reputed organizations across the world, including at Norton Healthcare (December 2023), Toronto Public Library (November 2023), Infosys (November 2023), and Indian Council of Medical Research (October 2023) vouch that such concerns are not at all misplaced.

Therefore, to protect consumers from unauthorized and illicit usage of their personal information, 137 countries have already enacted protection and privacy legislation in their respective countries.

Indian Context: Bharat is being celebrated for its DPI supremacy of initiatives like *Aadhar* and UPI, and is zealously propelled towards population-wide digital transformation of all its public services through several commendable initiatives, some of which are *Jeevan-Pranam* for pensioners, National Scholarship portal of India for students, shared digital healthcare infrastructure of National health stack (NHS) for all the citizens, e-*Sharam* platform for unorganized labour, agriculture data exchange platform (ADeX) for farmers and other stakeholders in agriculture ecosystem. This implies that the majority of its populace would soon become digital natives. During India's journey towards transformation driven by Artificial Intelligence, 'India Stack Global' has emerged as an influential instrument for both private and public entities to transition their services onto platforms within the nation. (Malhotra, 2024)[11]. It ensures faceless, cashless, presence less, and paperless transactions through its several layers including United Payments Interface (UPI), Aadhar (the unique digital identity of the residents in India), Digi-Locker (private space of digital natives in the public cloud), API-*Setu* (an interface for seamless exchange of data across platforms); as a result of which humungous personal data traverses through the digital platforms of service delivery organizations, making it a very popular tool of digitizing service delivery.

[11] Charru Malhotra (2024). Digital India- Past, Present and Future. In M. H.-P. Müller (Ed.), India in the 21st Century: On its way to a Post-industrial Economy. Springer Gabler. https://doi.org/10.1007/978-3-658-43014-6 (In Press)

For instance, in the last four years, digital payment transactions through the United Payments Interface-UPI layer of India Stack Global, increased by 326.8% in the financial year (FY) 2021-22 from FY 2017-18 (Source: RBI, NPCI, and banks as quoted in Press Information Bureau -PIB of India dated February 8, 2023). In this data journey, the fluid nature of data is a matter of concern; data is capable of quietly flowing in cross-border circulation as well as in internal ecosystems. The situation gets further complicated with the recent rapid proliferation of other New Age Technologies (NATs) including cloud computing, wearable devices with edge computing and so on that completely belie accountability or transparency to its end-users. These challenges of potential data breaches could fatally impinge on an individual's privacy. There could be threats to users' privacy in the wake of surging cyber threats of these data stores of personal data. Therefore, to protect privacy, ensure security, build trust, promote compliance, empower individuals, facilitate economic growth, and in alignment with international standards, India passed its Digital Personal Data Protection (DPDP) Act on August 11, 2023.

Review of the Literature: A review of the literature (for instance, Lynskey, 2023[13]) affirms that a Data Protection Act is crucial for safeguarding privacy, establishing security measures, and building trust between individuals and organizations. By the year 2017, 120 jurisdictions had comprehensive data privacy laws for the private sector, public sector, or (in most cases) both, and the laws meet at least minimum formal standards based on international agreements (Greenleaf, 2017[15]). By now, as per the United Nations Conference on Trade and Development (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide), 137 out of 194 countries have put in place legislation to secure the protection of data and privacy of their residents and 17 countries are ready with their respective draft legislation.

Literature (such as Bernal, 2016[17]) also cautions that it is improper to treat privacy as an individual right, but that it must be considered as a collective need for security. Such studies offer valuable insights into the broad implications of data protection laws, across different domains, illustrating their crucial role in safeguarding personal data while facilitating progress in scientific research and other fields. Privacy legislation

[13] Lynskey, O. (2023). Complete and effective data protection. Current Legal Problems, 76(1), 297–344. https://doi.org/10.1093/clp/cuad009

[15] Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Privacy Laws & Business International Report, (145), 14-18.

[17] Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. Journal of Cyber Policy, 1(2), 243-264.

provides a legal framework that ensures responsible data management, granting individuals control over their personal information while promoting accountability among organizations. Therefore, Sweeney (2001)[19] investigates data protection methods 'to safeguard identities in data' while still disseminating useful information. It emphasizes the need for establishing a balance between data utility and privacy, showcasing the challenges in anonymizing data effectively without losing its practical value. This body of work insists on establishing a formal framework for understanding disclosure control and explores several computational systems designed to maintain privacy in electronic data releases. Upholding the same concerns even, other authors (for instance, Binjubeir, Ahmed, Ismail, Sadiq & Khan, 2019)[21], have undertaken a critical comparative analysis of Privacy-Preserving Data Mining (PPDM) techniques that help in data modification to protect individual privacy while minimizing information loss for data analysis. The study discusses ongoing challenges and unresolved issues in the field of PPDM and underlines the importance of PPDM in sectors like banking, healthcare, and government, where large and complex data sets are common. Furthermore, privacy and data protection legislations support economic growth by fostering a secure digital environment that aligns with international standards, facilitating global business operations.

In context of Privacy legislation in India, several studies (such as Bailey, Bhandari, Parsheera & Rahman , 2018; Determann & Gupta, 2019)[25] provide an extensive critique of India's Draft Personal Data Protection (PDP) Bill (2018) and offer recommendations for revisions to ensure bill's compatibility with constitutional principles and global data protection standards especially with the GDPR and yet also emphasize the need for adapting compliance measures to address nuances specific to the Indian context (Prasad & Menon, 2020)[26]. Singh and Ruj (2020)[28]

[19] Sweeney, L. (2001). Computational disclosure control: A primer on data privacy protection (Doctoral dissertation, Massachusetts Institute of Technology).

[21] Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. IEEE Access, 8, 20067-20079.

[25] Binjubeir, M., Ahmed, A. A., Ismail, M. A. B., Sadiq, A. S., & Khan, M. K. (2019). Comprehensive survey on big data privacy protection. IEEE Access, 8, 20067-20079.
Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018). Comments on the (Draft) Personal Data Protection Bill 2018. National Institute of Public Finance & Policy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269735

[26] Determann, L., & Gupta, C. (2019). India's Personal Data Protection Act 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244203

[28] Prasad M, D., & Menon C, S. (2020). The Personal Data Protection Bill 2018: India's Regulatory Journey Towards a Comprehensive Data Protection Law. *International Journal of Law and Information Technology*. doi:10.1093/ijlit/eaaa003

offered a detailed technical analysis comparing it with European Union's GDPR and also explored cryptographic solutions for implementing the PDP Bill 2019, to successfully address challenges and limitations in its execution. Some of the authors (Charru Malhotra & Bhilwar, 2023)[30] critically evaluated the scope, provisions, and its impact on citizens' privacy rights, examining the balance between data protection, public interest, and state powers of Data Protection Bill –DPB of the year 2021 (DPB bill is the erstwhile version of DPDP). This study traced the evolution of data protection in India from its genesis of the Information Technology Act (ITA) 2008 (Amendment) till the phase of DPB, 2021. The paper further compared the DPB, 2021 with its predecessors and presented the challenges and opportunities of data protection legislation in India. Pirvan (2023)[32] too provides a comprehensive overview of India's evolving privacy rights and among other points, discusses various aspects of the DPDP Bill and its impact on various stakeholders as well as its implications on cross-border data transfers. There are also discussions to achieve both data protection and fair competition goals through data protection legislation (for instance, Srinivasan, Sinha & Modi, 2023). This study particularly illustrates how personal data regulation impacts antitrust enforcement and outlines necessary measures for the Competition Commission of India (CCI) in assessing digital antitrust cases in digital markets that are driven by data-centric business models. Korff (2023)[35] draws a comparison between the Indian DPDP Act 2023 and the European Union's GDPR, particularly in the context of international data transfers, data subject rights, and the scope of data processing. A study by Cook, Mariani, Kishnani, and Harr (2019)[37] also emphasizes the critical need for regulations to be adaptable, considering rapid technological changes and the globalized digital landscape.

Need for the study: The brief overview of the literature underscores the fact that the Privacy Act empowers users, mandates compliance, and protects against data misuse, playing a key role in the digital age. Therefore, there is

[30] Charru Malhotra & Bhilwar. A. (2024) Striving to Build Citizens' Trust in Digital World - Data Protection Bill (2021) of India; Technology, Policy, and Inclusion Technology, Policy, and Inclusion - An Intersection of Ideas for Public Policy (2024) ; Edited by Anjal Prakash, Aarushi Jain, Puran Singh and Avik Sarkar; Routledge , Taylor & Francis Group, London and New York (pp 141-161); DOI: 10.4324/9781003433194-6

[32] Pirvan, P. (2023). Safeguarding the Digital Frontier: An Overview of India's Privacy Rights and Digital Data Protection Bill 2023. DOI: 10.1732/IJLMH.25766

[35] Srinivasan, S., Sinha, V., Modi, S. (2023). Drafting a Pro-Antitrust and Data Protection Regulatory Framework. https://doi.org/10.55763/ippr.2023.04.05.003

[37] Cook, A. V., Mariani, J., Kishnani, P., & Harr, C. (2019). How to begin regulating a digital reality world. Deloitte Insights. Retrieved from (25.02. 2020): https://www2.deloitte.com/us/en/insights/industry/public-sector/regulating-digitalreality-augmented-spaces. html.

an exigent need for examining the national legal provision of the DPDP Act from the perspective of the ultimate beneficiary of these services *viz.* the digital natives. The present study attempts to demystify the DPDP Act of India with special reference to its key tenets, strengths, and limitations.

SECTION 2: CORE PRINCIPLES OF DPDP

India became the 19th G20 member nation to enact a comprehensive personal data law while serving as its G20 Presidency. DPDP Act strives to cause minimum disruption while ensuring necessary change in the way Data Fiduciaries process data; It is concise, lean, and SARAL, that is, Simple, Accessible, Rational & Actionable Law as it uses plain language; contains illustrations that make the meaning clear; contains no provisos ("Provided that…"); and has minimal cross-referencing.

Let us try to explore the basic nuances of the Act including its scope, basic provisions, and exemptions.

- **Definitions:** The Act defines crucial terms such as 'Data Fiduciary', 'Data Principal', 'Consent Manager', and 'Significant Data Fiduciary'. It also elaborates on what constitutes 'personal data', 'digital personal data', and 'personal data breach'.
- **Scope:** The Act applies to the processing of only personal data (and not non-personal, anonymized data), which is collected in digital form or in non-digital form that has been 'digitized' subsequently. It does not apply to 'non-automated', 'non-digital' personal data available in 'hard copy' etc.
- **Jurisdiction:** The DPDP Act applies to the processing of digital personal data within India and extends to processing outside India if it is related to offering goods or services to digital *natives* in India. It is not applicable in instances where the personal data is being shared for personal, domestic, legal, or official purposes without any commercial intent.
- **Provisions:**

1. **Data Fiduciaries:** Data fiduciaries (DF) are all the entities that handle (collect, store, process) the personal data of digital *natives* and operate in India. DF could be public as well as business entities, such as mobile app developers, internet service providers, and other companies. The Act lays down specific obligations/duties for them such as:

- Data processing is permissible only with the Data Principal's consent, with 'lawful purpose' being a prerequisite. They can process data without consent only when

the data principal voluntarily provides their data and does not indicate unwillingness to consent to its use.

- A verifiable consent is required from parents or legal guardians of children and specially-abled people for processing their data and exemptions to this are provided only in certain cases.
- The Act prohibits harmful or targeted data processing practices such as tracking, advertising, and behavioral monitoring targeted towards children or any other processing that is likely to cause any 'detrimental effect' on the well-being of a child.
- DF must make ensure the accuracy and completeness of the data and make reasonable and consistent efforts towards that.
- DF must erase personal data as soon as the purpose has been achieved and retention is no longer required for legal purposes.
- DF must put in place reasonable security safeguards to prevent a data breach
- DF must notify the Data Protection Board (DPB) of India and the affected individuals in the event of a breach, details of which would be intimated in the rules to the Act that is likely to be announced by the end of January 2024.
- **Cross-Border Transfers**: The Act allows personal data transfers for processing to all countries or territories outside Indian jurisdiction unless specifically barred by the government as a 'negative list' through notifications. The list is to be notified in the DPDP rules that are expected to follow.

2. **Significant Data Fiduciaries:** The Central Government may notify a fiduciary as a Significant Data Fiduciary (SDF), based on factors like data volume, sensitivity, and risks to the rights of the principals. SDFs must complete additional obligations and responsibilities such as:
   a. The appointment of a "Data processing agreement" is mandatory for them when they outsource activities to third parties.
   b. Must appoint a "Data Protection Officer" (DPO) who is based in India and is on the board of directors or similar governing body and serves as the first point of contact for grievance redressal.
   c. Must conduct periodic compliance measures including "Data Protection Impact Assessments (DPIA)" (is done on the controls/processing logic / technology stack/ any new solution/ app) and regular "risk audits" through "data auditors", as may be prescribed under rules.

3. **Data Processors: "**Data Processors" are entities or individuals that process personal data on behalf of the data fiduciaries such as cloud service providers, data analytics firms, and payroll processing companies. DF must ensure that these processors adhere to the requirements of the DPDP Act such as implementation of robust data protection measures, ensuring compliance with data processing standards mandated by the Act, maintaining documentation of processing instructions, and regularly monitoring the Processor's adherence.

4. **Data Principals:** The data principals (DP) have several Rights and Duties, some of the key ones are elaborated herewith.

   Rights of DP

   - **Consent:** DF has to take explicit consent from DP for processing their data for lawful and specific purposes. DF must take specific consent for all activities including to avoid unwarranted data processing, automated decision-making (such as awarding a loan), or profiling (to analyze or predict a person's performance at work, her reliability, or use of facial recognition technologies for school access and attendance control and so on). For example, if an online e-commerce platform has taken the personal data of the DP for the purchase of any household item, then the consent is exclusively applicable to only this transaction. This data of the DP cannot be transmitted to the parent company of that product and cannot be even shared with any other subsidiary of the e-commerce organization. This delimited, informed, and functional consent effectively is expected to safeguard the interests of the DP and prevent data misuse and other kinds of data threats mentioned afore. This is the key driving force of the Act.
   - **Access to Information:** DP has the right to access information about their data being processed, including the identities of those with whom their data is shared.
   - **Choice of Languages:** They can access information made available to them in English, or choose any language specified in the Eighth Schedule of the Constitution of India.
   - **Correction and Erasure:** They have the right to correct (say misspellings, change of address, etc.) complete, update, or erase their data, subject to legal constraints.
   - **Data Portability:** DP can port and hence reuse their data across diverse services, providing her convenience and better choices.

- **Grievance Redressal:** The Act provides for several grievance redressal mechanisms such as the DP can enter into mediation or initiate a complaint directly with the DF, if not satisfied with the DF can approach the Data Protection Board-DPB, then Appellate Tribunal, else seek legal redress through courts.
- **Nomination Right:** Right to nominate an individual to exercise rights on their behalf in the event of their death or incapacitation.

Duties of Data Principal

- Data Principals not to impersonate another person while providing personal data
- Data Principal must not suppress any material information while providing personal data
- Data Principal *is* not to register a false or frivolous grievance or complaint
- Data Principal to furnish only verifiably authentic information while exercising their right to data erasure.
- Data Principal to exhaust all the stipulated grievance redressal options before approaching the DPB.

5. **Consent Managers**: A consent manager (CM) acts as an intermediary between DF and DP to enhance transparency, confidence, and control of DP over their data. It could be a person or entity registered with DPB who shall serve as a single point of contact to assist DP in giving, managing, reviewing, and withdrawing their consent. This entire process is to be facilitated through an accessible, transparent, and interoperable platform.
6. **Data Protection Board (DPB) of India:** The Act stipulates the establishment of DPB of India, which serves as an adjudicatory body (and not a 'regulator') overseeing compliance and addressing disputes related to data processing. It can direct data fiduciaries to adopt urgent measures in case of data breaches and impose penalties for non-compliance. The DP can seek legal redress through the courts, as a final recourse, if not satisfied with DPB judgments. DPB can conduct hearings, summon and enforce attendance, and examine persons on oath, among other functions. The Board operates with the principles of natural justice and has powers akin to those of a civil court for matters related to summoning, receiving evidence, and document inspection. It is expected to function independently and would be composed of expert members drawn from various relevant fields. The government will designate its members. Board members will serve two-year terms with the possibility of reappointment.
7. **Appellate Tribunal:** Orders or directions issued by the Board can be appealed

before the Appellate Tribunal. Appeals must be filed within 60 days of receiving the order, and the Tribunal endeavors to dispose of appeals within six months. The orders passed by the Appellate Tribunal are executable as a civil court decree. The Tribunal can transmit orders to a local civil court for execution.

8. **Alternate Dispute Resolution:** The Act allows for mediation as an alternative dispute resolution mechanism, under the direction of the Board.

- **Implications**

  a. **Liabilities and penalties on data fiduciaries (DF):** DPDP imposes substantial financial penalties (and not criminal penalties) on DF to ensure adherence to data protection regulations

  - *Breach of Duty:* As mentioned above, DFs have specific duties/obligations under the Act, a breach of which can result in a penalty of up to INR Ten Thousand (INR 10,000).
  - Significant Data Fiduciary (SDF) has additional obligations, and non-compliance can lead to more severe penalties.
  - *Personal Data Breach:* In cases where data fiduciaries fail to implement security safeguards and a data breach occurs, they may face penalties up to INR Two Hundred Fifty crore (INR 250 crore).
  - *Breach Involving Children:* Any breach in observance of additional obligations related to children's data can attract penalties up to INR Two Hundred crore (INR 200 crore).
  - *Breach of any other provision of this Act* or the rules made thereunder Non-compliance shall lead to a penalty of INR 50 crore.

  b. **Penalty on data principal**: Breach in observance of the duties of the data principal shall lead to a penalty of INR 10,000.

- **Exemptions:** Some exemptions reflect a balancing nature of the DPDP Act, aiming to protect personal data while accommodating national security, legal, and practical considerations. Some of these are as below:

  i. *Exemptions to the State:* The Act allows certain exemptions to government organizations such as the data principals' rights to erasure and storage restrictions do not extend to government organizations.

  ii. *Processing of Children's Data:* The government may exempt certain classes of data fiduciaries and in certain scenarios, to

process children's data without all the obligations (such as obtaining parental consent or prohibiting behavioral monitoring) that are otherwise attached to the processing of children's data.

iii. *Security and Investigative Agencies:* Agencies processing data for India's integrity and sovereignty, national security, foreign relations, and public order, or to prevent incitement to any crime are exempt from certain provisions of the DPDP Act.

iv. *Research and Statistical Analysis:* Data processing required for statistical analysis, research, or archiving is exempt, if the data is not being used to make any decision specific to a data principal.

v. *Startups and Specific Data Fiduciaries:* Startups, may be exempt from notice, completeness, and accuracy, consistency, and deletion requirements by the government. This flexibility is likely aimed at encouraging innovation and growth, particularly for emerging businesses like startups, which might face challenges in meeting all the obligations under the Act due to their scale of operations and the nature of data processing activities.

vi. *Legal and Judicial Processes:* Exemptions are granted for processing necessary for/by enforcement of legal rights, court or tribunal activities, investigation or prosecution of offenses, etc.

vii. *Blockage of Information:* In the interests of the general public, Section 37 of the Act allows the government (or any authorized officer) to block public access to information of the data fiduciary's platform. This can occur if penalties have been imposed on the fiduciary on two or more occasions, or if the DPB recommends a blockage. However, the government must allow the data fiduciary to be heard before taking action. The government can order any intermediary to assist in giving effect to the blocking order.

viii. *Non-Indian Residents' Data:* Processing of data of a DP who is outside India / non-Indian residents, is exempt from the law's requirements regarding notice, consent, and obligations of data fiduciaries.

ix. *Government's Power to Demand Information:* The Act empowers the central government to call for information from the Board or from data fiduciaries or intermediaries for the purposes of the Act.

x. *Governments' Power to Notify*: The government can also notify certain data fiduciaries including startups that may otherwise be exempt from the Act, keeping in mind the volume and nature of personal data processed by them.

The exemptions indicate the Act's nuanced approach, recognizing that data protection needs to be flexible to adapt to various operational and national contexts.

- **Implementation**: The provisions of the Act are principle-based and high-level and the details around implementation will be set out in rules that are likely to be anounced by the end of January 2024.The Act, therefore, proposes a staged implementation, with the government notifying the clauses/rules that will take effect periodically.
- **Rules**: As is evident, the Act continues to give the Government broad powers to make subordinate rules or any other legislation or decisions on any aspect permitted under the Act. These rules could pertain to any aspect of the Act such as consent managers, process and format for reporting data breaches, matters related to the processing of children's data, significant data fiduciaries, and so on.

SECTION 3: KEY STRENGTHS OF DPDP

The Digital Personal Data Protection (DPDP) Act marks a significant milestone in India's legal landscape as the country's first statutory regulation dedicated to personal data protection. After over five years of meticulous deliberations, this Act emerges as a refined, lean legislative framework, distilled from a proposed 90 clauses to a concise 30, demonstrating its agility in adapting to the rapid advancements of new-age technologies. It equips the government with the authority to establish subordinate rules, offering a dynamic avenue for enhancing data privacy legislation in India. Notably, there are several reasons for celebrating the DPDP Act of India, some of which are listed herewith.

1. It is the first piece of statutory personal data protection regulation and represents the culmination of more than five years of deliberations and consideration.

2. It is a lean formulation with just 30 clauses (instead of the initially suggested 90 clauses in its previous avatar), making it

agile to changes wrought by rapidly evolving new-age technologies.

3. The Act provides the Government with the power to make subordinate rules, which presents a golden opportunity to upgrade the country's data privacy legislation. As a popular adage goes '*Perfection is an endless journey'*, therefore the possibility of enhancing the DPDP Act exists through subsequent framing of its subordinate rules.

4. It is one of the first Acts in India to be briefed using She/Her connotations.

5. Another strength of the Act lies in the insistence that it puts on data fiduciaries to adopt reasonable security safeguards to prevent personal data breaches and compulsory notifications it insists on if such breaches occur.

6. The Act seeks to provide a thorough framework for the processing of digital personal data in a way that respects each person's right to privacy protection as well as the necessity of processing such data for legitimate reasons of business interest and innovation.

7. Further, it has deftly inculcated foundational principles of 'Privacy by design' as well as 'Privacy by Default'. The former calls for the integration of data protection right from the onset of the designing of systems, which means privacy is embedded into the apps/device/systems design, processing & business practices, right from the outset. This has been inculcated by insisting on the conduct of Data Protection Impact Assessment- DPIA drills by significant data fiduciaries – SDFs (and not by start-ups) akin to EU-GDPR (Article 35) and to Singapore PDPA.

8. Similarly, the 'Privacy by default' principle too has been incorporated so that only the necessary personal data for each specific purpose may be processed, which has been imbued through the 'purpose limitation' approach. Both principles emphasize a preventive approach to data protection, ensuring compliance throughout the lifecycle of a project or system and not the level of the individual.

9. There are certain commendable steps such as the cross-border flow of the data has been liberalized to all the countries (except the blacklisted ones) and the imperative of 'data localization' has been done away with.

10. The load of 'consent fatigue' on the digital natives of India has been averted by not including the concept of 'additional consent'. However, this could become a double-edged sword; what would happen in the cases where the same data fiduciary (DF) has to process the data beyond the stated purposes? In the absence of a clear mention, how do we ensure that a DF won't misuse

the data on the sly or mislead her or the DPB?

SECTION 4: KEY CONCERNS ASSAILING DPDP

At present, one can note that the majority of the provisions of DPDP seem more supportive of the interests of the service-providing entities and not digital natives of India. Some other concerns of digital *natives*, as understood by the authors are stated herewith:

1. **How can a digital native give and alter her consent and in what circumstances?**

Given some of the concerns that assail from the perspective of digital natives can be summarized herewith.

a. How the consent would be taken from the digital native/data principal?

b. Would it be personalized and contextualized to her language, and her level of understanding? As per Section 6(2)(b), she must be given the option to access the contents of the notice, apart from English, in any of the 22 languages specified in the Constitution of India. It is a very reassuring mandate to her advantage but how would this be implemented is a moot concern.

c. Would she be aware of the circumstances when she has to initiate changes in her originally provided data or that she has to initiate the erasure of her data if the purpose of the original collection is no longer valid? For example, if she were working as an employee of the informal sector in urban areas and did not want to continue with a cab-hailing service that she had availed of just once, then how can she request the complete deletion of her data associated with the initial purpose of collection? Who would make her aware of all the circumstances when she has to initiate a data change, especially if she is, say, staying in a remote tribal village of the country and had given her data for applying for education elsewhere in the country?

d. Still worse, if this digital native had gullibly trusted someone else to fill her education form on her behalf and her details were inadvertently inaccurate; would she be fined INR 10,000 for 'supplying' inaccurate information?

e. Further, the Act does not regulate risks of harm arising from the processing of her data and the digital native does not even get any financial compensation if the breach of her data occurs.

2. **What happens to the personal sensitive data of digital natives?**

All the references to various categorizations of personal data to

"personal sensitive data" have been removed and the Act applies uniformly to both sensitive data and non-sensitive data, including sensitive personal data.

3. **Same issue and different opinions for the personal data of digital natives?**

   The lack of categorization of personal data into sensitive data and non-sensitive data is also not by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) SPDI Rules 2021. SPDI Rules categorize personal data into 'personal information' and 'sensitive personal data or information' unlike the DPDP Act.

4. **Where would the personal data of digital natives be stored?**

   The fact that the DPDP Act allows data to flow freely to any country (except those on a 'negative list' to be specified by the government) is very liberating. However, the Act does not explicitly insist either on data localization or on its storage outside India. What is the implication of this ambiguity?

5. **Is DPB empowered to support the cause of hapless digital natives?**

   The establishment of an authoritative body is provided but the presently suggested DPB is very different from the initially proposed regulatory institutional framework of DPA (PDP, 2018/2019). The erstwhile Digital Protection Authority (DPA) of India- suggested DPDP was arguably more potent and had more regulation-making powers than even DPAs suggested under EU-GDPR. Apart from looking into noncompliance instances, it had been bestowed with powers of formulating legislation, tasked with creating business codes of conduct, gathering supervisory data, and implementing fines on companies (Charru Malhotra & Bhilwar, 2024).

   a. However, in its present format, DPB is not a regulatory body and is restricted to only supervising data breach prevention, ordering corrective action, conducting investigations, and imposing fines for legal non-compliance.
   b. It lacks the authority to request information to monitor how enterprises run, or to issue binding regulations, rules, or conduct codes, which may limit its ability to address emerging issues and challenges in the data protection landscape.
   c. The board is composed of six members and a chairperson, all of whom are appointed by the Central Government on the recommendation of a selection

committee. This may raise concerns about the potential influence of the government on the DPB's decisions and actions.

d. Further, only one member is supposed to be a legal expert.
e. The act also fails to specify and preserve an internal separation of functions between the members conducting inquiries and the authority of the chairperson.
f. The DPB's chairperson is empowered to authorize any board member to execute "any of the functions of the board and conduct any of its proceedings" which might not prove to be an impartial process.

6. **Privacy rights of digital natives (im)balanced against the rights of the state to safeguard national security?** DPDP has provisions for processing personal information without consent for national security purposes. There is a catch-22 situation of various sorts here. A lot will depend upon how well the government upholds privacy rights especially since the central government has a huge amount of discretionary control over substantive matters such as:

a. Section 7(b) of the Act permits the government to circumvent consent requirements in cases where a beneficiary of government services has already been permitted to receive any other benefit from the state. To fully utilize this provision, government entities need to be freed from purpose limitation that mandates that personal data be erased once its intended use has been fulfilled.
b. However, in another provision of Section 17(2)(a) certain state agencies have been absolved from consent mechanisms. Although there are situations where this is justified, such as during emergencies or disasters, but the legislation expands the range of these situations and the state gains considerable power over the digital *natives*.
c. Further, Section 17(5), of the Act gives power to the Central Government to exempt any data fiduciary from complying with any part of the Act for a certain period, not exceeding five years from the date of commencement of the Act in the interest of sovereignty and integrity of India,

the security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence relating to the above matters. The fear remains that in certain situations, the government's freedom may work against the privacy safeguards or the interests of the digital natives.

d. Similarly, the government can exclude companies from various regulations governing the handling of children's data by using its arbitrary rule-making powers.

7. Has DPDP diluted the Right to Information (RTI) of digital natives?

The Act seeks to amend the 2005 Right to Information Act (RTI Act) by removing the requirement for personal data disclosure to be tied to public interest. This is a huge drawback to the Act's implementation in various ways as listed herewith:

a. **Exemptions and Personal Data:** Under the RTI Act, Section 8(1) (j) exempts personal information from disclosure, unless it relates to public activity or interest, or its disclosure is justified by larger public interest. The DPDP Act, with its emphasis on protecting personal data (Sections 3 to 14 outlining the rights and duties of data principals and fiduciaries), strengthens the protection of personal data. This enhanced protection could make public authorities more cautious in releasing personal data under the RTI Act, potentially leading to a narrower interpretation of what constitutes 'public activity or interest'.

b. **Data Protection vs. Public Interest:** The RTI Act's objective is to promote transparency and accountability (Section 3 provides the right to information), while the DPDP Act is geared towards protecting personal data against processing that is harmful to individuals (Sections 3 to 14 detail various protections). The two objectives could conflict when an RTI request seeks information that includes personal data protected under the DPDP Act. Balancing public interest against personal data protection might lead to more conservative disclosures under the RTI Act.

c. **Bureaucratic Processes:** The DPDP Act introduces compliance requirements for data fiduciaries (Sections 8 and 10 outlines the general obligations and additional obligations for significant data

fiduciaries), which could add layers of bureaucratic review for RTI requests involving personal data. This might lead to delays or additional hurdles in the RTI information request process, especially where personal data is involved.

d. **Overlap in Appeals and Oversight Bodies:** The RTI Act establishes Information Commissions at the Central and State levels (Sections 12 and 15) as appellate authorities, while the DPDP Act establishes the Data Protection Board of India (Sections 18 to 28) to oversee compliance and resolve grievances related to data protection. This creates two parallel redressal mechanisms, which could lead to jurisdictional overlap or confusion, particularly in cases where an RTI request for information involves personal data protected under the DPDP Act.

8. Last but not least, India patronizing its startups too much, is what we need to rethink and reconsider to safeguard the interests of digital natives.

Needless to say, this list is not an exhaustive one and may be considered merely the tip of the iceberg. Digital natives are expected to have a comprehensive knowledge of the different provisions of the DPDP as well as if their respective service providers are adhering to them. How would the scale and diversity of the Indian context be coped with is still unclear?

SECTION 5:KEY RECOMMENDATIOS

As is obvious from the previous section (Section 4), well-laid implementation strategies are still awaited for the Act which could help to truly achieve the primary objective of safeguarding the interests of the digital natives. Respecting the profile of our digital native, the authors, therefore, strongly suggest that these data protection measures should also be inculcated as an essential part of the startups from the very beginning. A balance of priorities must ensue. The idea is not to stifle technology but to safeguard the interests of our digital natives. Further DPDP needs to stay updated with technological progress and worldwide changes. Even the global landscape of data privacy laws and new data protection legislations are constantly evolving by new age technologies (NATs). This adaptability proves essential in evolving guidelines in harmony with technological progress to support the interests of the unassuming digital natives. Adaptive regulation, regulatory sandboxes, and outcome-based approaches are some of the methods that could be inculcated to ensure that the DPDP Act and its ensuing Rules keep pace with technological advancement and effectively address the complexities of digital privacy and security.

CONCLUDING REMARKS

Personal data is sacrosanct, and it is essential to protect it. The emergence of New Age Technologies, particularly AI's interference with personal data without accountability has led to societal concerns. Therefore, legislation of the DPDP Act 2023 of India is a small step in the right direction. The Act has assumed a flexible approach that allows for regular rule updates to its law in response to technological advancements and societal changes. It upholds the rights of digital natives and has set newer standards and additional insistences on service delivery entities, particularly the ones that would be deemed more 'significant'. The contradiction comes whether to use the law to merely protect the privacy of over a billion digital natives or to use it efficiently to propel its digital economy or further enhance national security. The proposed act must align with global trends and India's inclusive technology approach to ensure equitable access for its diverse population while advancing its journey toward *Viksit Bharat* @ 2047 which is the nation's dream of achieving a self-reliant progressive India by the year 2047.

Understanding Digital Data Protection

Sh. Anoop Kumar Verma, Sr. Administrative Officer, O/o C&AG of India

Mr. Anoop Kumar Verma is currently working as Sr. Administrative Officer in Report Central Wing of the CAG's Headquarters. He has the experience of auditing computer billing system of DISCOM during his posting at Lucknow. He also has experience of working on data relating to General Insurance company during his posting at MAB-II, New Delhi.

The article emphasizes the critical importance of digital data protection in an increasingly interconnected world. It outlines the evolving threats to digital data, including cyber risks and data privacy concerns, and discusses key principles for safeguarding sensitive information, such as encryption, access control, and employee training. The article also reviews the regulatory landscape, highlighting significant laws like India's Digital Personal Data Protection Act, 2023, and international frameworks like the GDPR and CCPA. Ultimately, it calls for comprehensive security measures and awareness to create a secure digital ecosystem and protect individual privacy.

In the present era dominated by technological advancements and a digitalized landscape, the protection of digital data has become a paramount concern for individuals, businesses and governments alike. As the world increasingly relies on digital platforms and interconnected systems, the need for robust data protection measures has never been more critical. In this article, we will understand the digital data and explore the importance of digital data protection, the evolving threats and relevant legislations along with strategies to safeguard sensitive information in the digital realm.

Let us understand the term first- Data refers to raw, unprocessed facts, figures, symbols, or information. It is a broad term that encompasses qualitative or quantitative values, and it can represent anything from numbers and text to images, sounds, and more. It is important to note that the term "data" is plural, while "datum" is the singular form. The data may be either quantitative or qualitative. Additionally, it may also be structured or unstructured data.

The **Digital Data** is 'the electronic representation of information in a format or language that machines can read and understand'. In technical terms, digital data refers to information that is represented in a numerical or binary format, typically using combinations of 0s and 1s. The power of digital data is that any analogue inputs, from very simple text documents to genome

sequencing results, can be represented with the binary system.

Digital data encompasses a wide range of information, including personal, financial, and business-related data. The significance of digital data protection cannot be overstated, as breaches can lead to severe consequences such as identity theft, financial loss, and compromise of intellectual property. As technology continues to advance, so do the methods employed by cybercriminals, making it imperative for individuals and organizations to stay one step ahead in securing their digital assets.

Evolving Threat Landscape

The digital landscape is fraught with various threats. Digital risks include cybersecurity risks, third-party risks, and data privacy risks ranging from malware and phishing attacks to ransomware and data breaches. Cybercriminals continuously adapt and refine their tactics to exploit vulnerabilities in systems and networks. With the increasing interconnectivity of devices through the Internet of Things, the attack surface expands, making it more challenging to protect sensitive information. Therefore, understanding the evolving threat landscape is crucial for implementing effective digital data protection measures.

Key Principles of Digital Data Protection

- **Encryption:** Utilizing strong encryption algorithms is fundamental to securing digital data. Encrypting data at rest and in transit ensures that even if unauthorized individuals gain access, the information remains unreadable and unusable without the proper decryption keys.
- **Access Control:** Implementing robust access control measures helps restrict access to sensitive data. Assigning appropriate access privileges to individuals based on their roles and responsibilities ensures that only authorized personnel can view or modify specific information.
- **Regular Audits and Monitoring:** Conducting regular audits of digital systems and monitoring for unusual activities can help detect potential security breaches early on. Timely identification of anomalies allows a swift response to mitigate potential risks.
- **Data Backups:** Regularly backing up digital data is a crucial component of data protection. In

the event of a cyberattack or system failure, having up-to-date backups ensures that information can be restored, minimizing potential data loss.

- **Employee Training and Awareness:** Human error is a significant factor in data breaches. Providing comprehensive training to employees on security best practices and raising awareness about potential threats can contribute to a more secure digital environment.

Regulatory Framework

In our interconnected world, where digital data flows seamlessly across borders, the need for comprehensive data protection laws has become increasingly evident. Governments worldwide have recognized the importance of safeguarding individuals' privacy and ensuring the responsible handling of personal information and Governments and regulatory bodies around the world are enacting stringent data protection laws to hold organizations accountable for safeguarding personal information. Compliance with regulations is essential for avoiding legal consequences and maintaining trust with stakeholders.

The landscape of digital data protection laws is dynamic and reflects a global effort to address the challenges posed by the digital age. While these regulations vary in scope and stringency, they collectively underscore the importance of respecting individuals' privacy and ensuring responsible data handling practices. For businesses and organizations operating across borders, understanding and complying with these diverse regulations are essential to maintaining trust, safeguarding sensitive information, and navigating the complex terrain of the global digital economy.

Except few countries[39], almost all the countries (including India) have legislations relating to data protection or in the process[40] of adopting it. Just look at the global landscape for these regulatory frameworks:

India-Personal Data Protection Act, 2023

The legislation incorporates elements of user consent, data localization, and the establishment of a Data Protection Authority to oversee compliance. This will protect digital personal data by providing the obligations of Data Fiduciaries for data processing, rights and duties of Data Principals and financial penalties for breach of rights, duties and obligations. This law also seeks to achieve data protection law with

[39] Libya, Sudan, Afghanistan, Venezuela, Bangladesh, Sri Lanka to name a few
[40] Pakistan, Saudi Arabia, Ethiopia, Iraq

minimum disruption while ensuring necessary change in the war Data Fiduciaries process data.

The Digital Personal Data Protection (DPDP) Act, 2023 applies to the processing of digital personal data within the territory of India collected online or collected offline and later digitized. It is also applicable to processing digital personal data outside the territory of India, if it involves providing goods or services to the data principals within the territory of India.

DPDP Act underlines the role of significant data fiduciary (SDF), which the government will identify using the volume and sensitivity of personal data processed and risk associated. The specific obligations under this include appointing a data protection officer based in India; appointing an independent data auditor; and conducting a data protection impact assessment.

European Union-General Data Protection Regulation

The regulation, implemented in May 2018, applicable to all EU member states. It focuses on empowering individuals with greater control over their personal data and imposes strict obligations on organizations that process such information. GDPR enforces principles such as data minimization, purpose limitation, and the right to be forgotten, with severe penalties for non-compliance.

United States of America- California Consumer Privacy Act

Enacted in 2020, the CCPA is a state-level regulation in the United States, but its influence extends far beyond California due to the state's economic significance. The CCPA grants California residents the right to know, delete, and opt-out of the sale of their personal information. It applies to businesses meeting specific criteria, including those that process large amounts of consumer data.

China- Personal Information Protection Law

This law, effective from November 2021, focuses on regulating the processing of personal information by both government and private entities. It introduces concepts such as "important data" and "cross-border transfers," requiring businesses to conduct assessments before transferring certain data outside of China.

Australia- Privacy Act, 1988

This law amended in 2021, include the Notifiable Data Breaches scheme, which mandates organizations to report significant data breaches to the Office of the Australian Information Commissioner and affected individuals. It also introduces enhanced penalties for non-compliance.

Conclusion

As our dependence on digital technologies continues to grow, so does the need for robust digital data protection. Understanding the evolving threat landscape and implementing comprehensive security measures are essential for individuals, businesses, and governments to navigate the digital realm safely. By adhering to key principles and staying informed about regulatory requirements, we can collectively contribute to creating a secure and resilient digital ecosystem. This is more important in respect of personal data. Implementing practical measures for personal data protection is not only essential for preserving individual privacy but also for maintaining a secure and trustworthy online environment. By staying informed, practicing vigilance, and adopting good cybersecurity habits, individuals can significantly reduce the likelihood of falling victim to data breaches and identity theft, ensuring a safer digital experience.

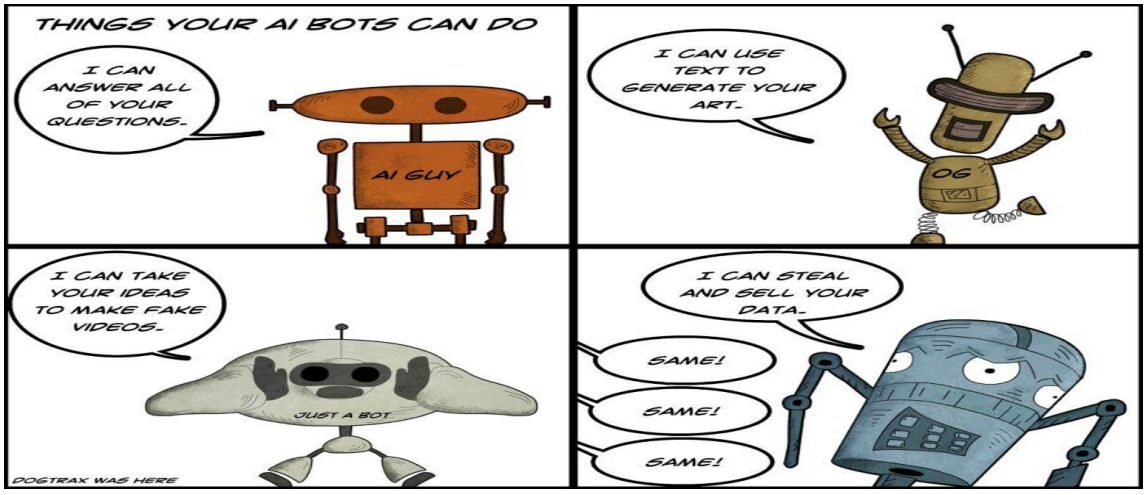
References:

https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264

https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

https://www.ey.com/en_in/cybersecurity/decoding-the-digital-personal-data-protection-act-2023



Reference: https://www.flickr.com/photos/dogtrax/52844938164

Digital Data Protection

Sh. Sant Vijay Singh, AAO, iCISA Noida

Shri Sant Vijay Singh is currently working as Assistant Administrative Officer in Budget, Infra and IS section of iCISA, Noida.

The article highlights the critical importance of digital data protection in India, emphasizing the surge in internet users and the growth of the digital economy. It discusses the various dimensions of digital data, including its role in individual privacy, economic growth, social development, and national security. The piece outlines the threats to digital data, such as cybersecurity risks and privacy concerns, while advocating for robust data protection measures to empower individuals, foster trust in digital platforms, and ensure a secure digital environment.

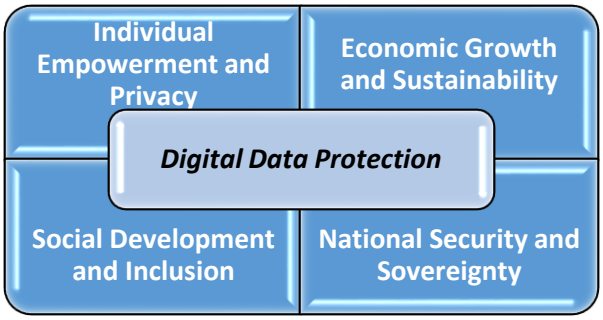
Digital data holds immense significance and drives various aspects of life, from individual interactions to government initiatives. It refers to any information created, stored, and communicated in digital form. This includes text, images, videos, audio recordings, social media posts, financial transactions, government records, and much more. In essence, it's any information represented electronically.

India has witnessed a massive surge in internet users, reaching over 830 million. This has fuelled the growth of the digital economy, with sectors like e-commerce, digital payments, and online education flourishing. Data plays a crucial role in these sectors, enabling platforms to personalize experiences, improve services, and drive innovation.

The Indian government's "Digital India" initiative promotes data-driven governance and leverages digital infrastructure to deliver citizen services more efficiently. Examples include Aadhar (unique identification system), e-KYC (electronic Know Your Customer), and various online portals for accessing government services. From online banking and shopping to social media interactions, digital data permeates personal lives in India. Individuals generate data through their online activities, which can be used for targeted advertising, personalized experiences, and even credit scoring.

Aspect	Description	Example	Impact	Challenges
Definition	Information created, stored, and communicated electronically	Text, images, videos, transactions	Drives various aspects of life	
Growth	Massive surge in internet users (830 million+)	E-commerce, digital payments, online education	Boosts digital economy	Digital divide
Government	"Digital India" initiative for data-driven governance	Aadhaar, e-KYC, online portals	Efficient citizen services	Privacy concerns
Individuals	Permeates personal lives through online activities	Social media, banking, shopping	Personalized experiences, financial access	Security risks
Overall	Immense significance, but requires balancing opportunities and challenges		Growth, innovation, inclusion	Privacy, security, ethics

Digital Data Protection is need of hour:



The surge in internet users and digital adoption in India necessitates robust data protection measures for several reasons.

1. **Individual Empowerment and Privacy:**
   - Right to privacy: Digital data encompasses personal information, and its protection aligns with the fundamental right to privacy enshrined in the Indian Constitution.
   - Control over personal data: Individuals deserve control over how their data is collected, used, and shared. Data protection empowers them to make informed choices and prevent misuse.
   - Mitigating risks: Unprotected data exposes individuals to privacy violations, identity theft, financial scams, and discrimination based on personal information.
2. **Economic Growth and Sustainability:**
   - Building trust in the digital economy: Data breaches and privacy scandals erode trust in digital platforms and hinder online transactions, impacting e-commerce, digital payments, and other sectors.
   - Protecting intellectual property: Sensitive data related to businesses, innovations, and trade secrets needs protection to encourage investment and fair competition.
   - Cybersecurity resilience: Strong data protection practices enhance cybersecurity, reducing business disruptions and financial losses due to cyberattacks.
3. **Social Development and Inclusion:**
   - Promoting responsible innovation: Data-driven initiatives in healthcare, education, and social welfare require ethical frameworks to ensure data security and prevent discrimination.
   - Bridging the digital divide: Addressing data privacy concerns can encourage participation from vulnerable populations hesitant to engage in the digital space due to privacy fears.
   - Combating online harms: Data protection measures help tackle cyberbullying, online harassment, and the spread of misinformation, fostering a safer online environment.

4. **National Security and Sovereignty:**
    - Protecting critical infrastructure: Data related to national security, defense, and essential services needs robust protection from cyber threats and foreign espionage.
    - Countering cybercrime: Strong data protection laws and international cooperation help combat cybercrime across borders, ensuring national security and international stability.
    - Data localization: Balancing the need for global data flows with safeguarding sensitive information within India's borders is crucial for maintaining national sovereignty.

Threats to Digital Data:

1. Cybersecurity Threats:

- Evolving Attack Landscape: Cybercriminals constantly develop new attack methods, making it challenging for organizations and individuals to stay ahead. Phishing emails, ransomware attacks, and zero-day exploits become increasingly sophisticated.
- Mass Data Breaches: Large-scale data breaches expose millions of records, compromising personal information like financial details, healthcare data, and even Aadhaar credentials. Recent examples include leaks from Air India and MobiKwik.
- Targeted Attacks: Critical infrastructure, government agencies, and businesses face targeted attacks from state-sponsored actors or cybercriminals seeking strategic advantages.
- Internet of Things (IoT) Vulnerabilities: The growing deployment of connected devices opens new attack vectors. Unsecured IoT devices can act as entry points for attackers to infiltrate networks and access sensitive data.

2. Privacy Concerns:

- Lack of Awareness: Many individuals remain unaware of data privacy risks and how their online activities generate data trails. This makes them vulnerable to targeted advertising, identity theft, and manipulation.
- Inadequate Data Protection Laws: While the DPDPA is still evolving, concerns remain regarding its effectiveness in addressing emerging challenges and providing robust enforcement mechanisms.
- Government Surveillance: Concerns exist about potential misuse of surveillance programs and the lack of

clear legal frameworks regulating data collection and access by government agencies.

- Social Media Data Exploitation: Social media platforms collect vast amounts of personal data, raising concerns about targeted profiling, manipulation, and potential breaches compromising sensitive information.

3. Other Threats:

- Digital Divide: Unequal access to technology and digital literacy limits awareness and capabilities to protect data. This excludes a significant section of the population from the benefits of a digital society while leaving them vulnerable to exploitation.
- Skill Gap in Cybersecurity: India faces a shortage of skilled cybersecurity professionals, hindering its ability to effectively respond to evolving threats and manage data security infrastructure.
- Outdated Infrastructure: Legacy systems and outdated technology in some sectors create vulnerabilities that attackers can exploit to gain unauthorized access to critical data.

Instances of digital data breaches:

Unfortunately, data breaches are becoming increasingly common in India, affecting both individuals and organizations. Here are some notable examples from the past 4 years:

- Air India (February 2021): Personal information of 4.5 million passengers leaked, including passport numbers, phone numbers, and email addresses. (https://www.businesstoday.in/latest/trends/story/exclusive-if-you-flew-air-india-your-data-could-be-compromised-346626-2022-09-07)

- Dominos India (May 2021): Over 18 crore orders leaked, including customer names, addresses, phone numbers, and even credit card details for 1 million individuals. (https://indianexpress.com/article/technology/tech-news-technology/dominos-data-breach-name-address-other-details-of-over-18-crore-orders-leaked-7328416/-name-address-other-details-of-over-18-crore-orders-leaked-7328416/)

- SBI Data Breach (2019): Unprotected server of SBI that allowed anyone to access financial information on millions of its customers, like bank balances and recent transactions. (https://techcrunch.com/2019/01/30/state-bank-india-data-leak/).

- MobiKwik Breach (2021): Data of over 3.5 million users leaked, including phone numbers, email addresses, and transaction details. (https://www.thehindubusinessline.com/info-tech/data-of-35-m-mobikwik-users-allegedly-hacked/article34192591.ece)

- Unacademy Data Breach (2020): Data of over 20 million users leaked, including names, email addresses, and phone numbers. (https://www.business-standard.com/article/companies/unacademy-s-database-hacked-information-of-11-million-users-compromised-120050701280_1.html)

Consequences of Digital Data breach:

Data breaches are not merely technical glitches; they have far-reaching consequences that impact individuals, businesses, and societies as a whole. Understanding these consequences is crucial for implementing effective data protection measures, promoting responsible data practices, and building a more secure digital future for all.

1. Financial Fraud:

- Identity Theft: Stolen personal information like names, addresses, and Social Security numbers can be used to open fraudulent bank accounts, credit cards, or loans, leaving victims responsible for the debt.
- Financial Transactions: Payment card details or bank account information can be used for unauthorized purchases, draining victims' financial resources.
- Tax Fraud: Stolen information can be used to file fraudulent tax returns, leaving victims liable for additional taxes and penalties.

2. Personal Harm:

- Stalking and Harassment: Online information like location data, social media profiles, and contact details can be used to stalk, harass, or even threaten individuals.
- Reputation Damage: Leaked personal information or embarrassing content can be used to damage someone's reputation online or offline, impacting their personal and professional life.
- Discrimination: Sensitive information like health records or political affiliation can be used to discriminate

against individuals in areas like employment, housing, or insurance.

3. Social Manipulation:

- Targeted Propaganda and Misinformation: Stolen data can be used to create personalized profiles and target individuals with fake news, propaganda, or manipulative content, influencing their opinions and actions.
- Election Interference: Voter information and demographics can be misused to influence elections through targeted campaigns, suppressing turnout, or spreading disinformation.
- Social Unrest: Stolen data can be used to sow discord and manipulate public opinion, potentially leading to social unrest or violence.

4. Business Disruption:

- Competitive Advantage: Stolen trade secrets, intellectual property, or customer data can give competitors an unfair advantage, harming businesses financially.
- Ransomware Attacks: Attackers may encrypt business data and demand ransom payments, disrupting operations and causing financial losses.
- Supply Chain Disruptions: Compromised data in critical sectors like energy or transportation can lead to widespread disruptions and economic damage.

5. National Security Threats:

- Espionage: India's Digital Personal Data Protection Act (DPDPA): Enacted in 2023, this law aims to regulate personal data collection, storage, and processing by organizations operating in India.

Auditing Digital Data in India:

The increasing digitization of India across various sectors has led to a surge in digital data generation and storage. This brings immense benefits but also significant risks requiring robust data security measures and effective auditing practices. Here's a comprehensive guide to auditing digital data in India:

1. Understanding the Landscape:

- **Regulatory Framework:** Familiarize with relevant regulations like the Digital Personal Data Protection Act (DPDPA), industry-specific

guidelines, and international standards like ISO 27001.

- **Data Sensitivity:** Classify data based on its sensitivity (personal, financial, etc.) to prioritize audit focus and implement appropriate controls.
- **Organizational Context:** Understand the organization's data ecosystem, including technologies, processes, and stakeholders, to tailor the audit approach.

2. Key Audit Areas:

- **Data Governance and Management:**
  - Assess data collection, storage, retention, and disposal practices.
  - Evaluate access controls and user authentication mechanisms.
  - Review data lifecycle management policies and procedures.
- **Cybersecurity Posture:**
  - Identify and address vulnerabilities in systems, networks, and applications.
  - Evaluate security patching, intrusion detection, and incident response capabilities.
  - Assess the effectiveness of security awareness training for employees.
- **Third-Party Risk Management:**
  - Evaluate the data security practices of third-party vendors and partners.
  - Ensure contractual agreements include adequate data protection clauses.
  - Monitor their security practices through ongoing assessments.
- **Compliance Verification:**
  - Assess compliance with relevant data privacy regulations and internal policies.
  - Identify and address compliance gaps and potential risks.
  - Prepare necessary documentation and reporting evidence.

3. Key Considerations for Effective IT Audits:

- **Leveraging Technology:** Utilize data analytics tools and automation to improve audit efficiency and effectiveness.
- Scope and methodology: Tailor the audit to specific organizational needs and risk profiles.
- Auditor expertise: Choose qualified and experienced professionals with relevant data security knowledge.
- Continuous monitoring and improvement: Regular audits and ongoing efforts are essential for staying ahead of evolving threats.
- Cloud Security Assessments: Address specific security considerations related to cloud-based data storage and processing.
- **Human Factor Consideration:** Address human error risks through employee training and awareness programs.

By leveraging IT audits effectively, organizations can gain valuable insights into their digital data security posture, identify and address vulnerabilities, and ultimately protect their valuable information from a range of threats.

There is need of a multi-pronged approach to navigate the complexities of digital data in India. We must strike a balance between harnessing the power of digital data and mitigating its risks to privacy, security, and social equity. Both individuals and organizations must be vigilant about data protection, practicing good online hygiene and implementing appropriate security measures. Educating individuals about their data rights and empowering them to make informed choices are essential for a healthy digital ecosystem. Further, regular audits by qualified professionals can help identify and address vulnerabilities in data security practices, fostering a culture of continuous improvement.

Decoding String-Matching Methods

By Sh. Anil Kumar Goyal, Sr.AO (CDMA), O/o C&AG of India

Mr. Anil Kumar Goyal is a Senior Administrative Officer at the CDMA Wing in O/o the C&AG of India, New Delhi. With a B.Sc. and M.Sc. degrees, he has 25+ years experience in auditing projects, analyzing government finance accounts, and conducting data analytics for major initiatives like PM Kisan Samman Nidhi and Ayushman Bharat.

The article explores the crucial role of string matching in Natural Language Processing (NLP) and its applications in data analytics. It discusses various algorithms, including lexical methods like Levenshtein distance and phonetic approaches like Soundex and Metaphone, which help compare and match text strings effectively. Emphasizing their importance in audits and data integrity, the article highlights how these methods are essential for safeguarding sensitive information in an increasingly digital world.

Ever wondered how a search engine can provide accurate results even with spelling mistakes? Or marvelled at its ability to predict searches with just a few characters entered? While numerous advanced analytics and artificial intelligence algorithms contribute to these feats, Natural Language Processing (NLP) plays a crucial role in this recipe. NLP, a subset of artificial intelligence, focuses on facilitating communication between computers and human language. Its primary objective is to empower machines to comprehend, interpret, and generate language akin to human communication in a meaningful and contextually relevant manner. While we won't delve deeply into NLP, it's worth noting that text analytics or string matching is a fundamental task within NLP analytics.

Now, let's shift our attention to string matching. Comparing strings isn't as straightforward as comparing numeric fields due to the complexity inherent in the nature of string matching. While numeric fields benefit from various statistical methods for comparison, matching text strings constitutes a common and fundamental task in many text-processing algorithms.

The primary goal of string similarity algorithms is to quantify the likeness between two text strings using string metrics. Often, text or string matching is interchangeably referred to as fuzzy matching, although the term "fuzzy match" encompasses a broad range of tasks, including comparing numbers using fuzzy matching. Think back to elementary school when we were told that the value of pi (π) could be approximated as 22/7, acknowledging a degree of imprecision a fuzzy match.

Fuzzy matching problems involve inputting two strings and generating a score that quantifies the likelihood that they represent the same entity. For instance, "Geeta" and "Gita" or "Geetha" should yield a high score, while a comparison between "Apple" and "Microsoft" should not. Over the years, various algorithms for fuzzy string matching have emerged, each with its strengths and weaknesses. These algorithms broadly fall

into two categories: lexical matching and phonetic matching.

Lexical Matching Algorithms:

Lexical matching algorithms operate based on models of errors, specifically designed to handle strings differing due to spelling or typing errors. Take, for instance, the comparison between "atharv" and "ahtarv." A lexical matching algorithm would recognize the transposition of "ht" and "th," a common error in typing. Algorithms in this category are often classified as either "edit distance-based" or "token-based." One of the most popular algorithms falling in this category is 'Levenshtein algorithm'.

Levenshtein Method

Named after Vladimir Levenshtein, this algorithm calculates the minimum number of single-character edits (insertions, deletions, or substitutions) required to transform one word into another. The Levenshtein distance is a fundamental measure in string matching, often referred to as edit distance.

For example, Levenstein distance between 'Ram' and 'Rama' (which is another form of spelling Ram especially in transliterated Sanskrit texts) is 1 because it involves one edit (insertion) only. On the other hand, Levenstein distance between 'Geeta' and 'Gita' is 2 (1 deletion and 1 insertion). One interesting thing to note here is that, this distance is case sensitive and therefore the distance between 'Geeta' and 'gita' is 3 instead of 2 (as it involves one extra substitution).

Note that this distance results in a number which can have integer value ranging upto number of characters in lengthier string.

Let us also discuss some other algorithms for lexical matching of two strings.

Hamming Distance:

Computed by overlaying one string onto another, hamming distance, named after mathematician Richard Hamming, identifies places where the strings differ. While originally intended for strings of the same length, some implementations handle variations by adding padding at the prefix or suffix.

So, calculating hamming distance between 'geeta' and 'gita' or 'Ram' and 'Rama' is fundamentally not possible. Moreover, like Levenshtien method this algorithm depends upon case therefore hamming distance between 'Geeta' and 'githa' would be 4 as it involves four changes.

Jaro-Winkler: Method

Jaro-Winkler algorithm gives high scores to two strings if they contain the same characters within a certain distance from one another and if the order of matching characters is the same. This algorithm is directional and rewards high

scores for matches from the beginning of the strings. Actually Jaro-Winkler was extension of Jaro distance which did not take into account the match from beginning of the string.

Like previous two algorithms, this one is also named after two statisticians Matthew Jaro and William Winkler. However, unlike previous two algorithms, this algorithm gives normalised score i.e. a value between 0 (which means exact match) and 1 (meaning not matching).

So, JW distance between 'atharv' and 'ahtarv' would be greater (0.05) than that between 'atharv' and 'athrav' (0.038) despite have one transposition in both the sets. As can be seen that the distance is larger if the transposition is near to beginning of strings.

Q-Gram:

Q-Gram, based on the difference between occurrences of Q consecutive characters in two strings, is effective for understanding similarities. It forms unique Q-grams in each string and measures the overlap, making it valuable for certain types of string matching.

To understand the algorithm, let us take a look at special case where Q = 3. String say 'abcd' has two 3-grams i.e. 'abc' and 'bcd'. So, string distance on Q-gram based algorithm would be number of different q-grams out of total unique q-grams. The distance based on this method between 'Geeta' and 'Gita' would be 5.

Phonetic Matching Algorithms:

Phonetic matching algorithms are designed to compare strings by their similar sound patterns, allowing for effective matching even when there are differences in spelling.These algorithms prove useful in scenarios where the comparison involves non-grammatical words, such as names of individuals or companies.In contrast to lexical matching algorithms that yield a metric when comparing two strings, phonetic algorithms typically generate a specific code for each string or word. Additionally, it's important to note that these algorithms exhibit variations in their functionality across different language settings.

Soundex:

Created in 1918, Soundex matches words based on the rules of English pronunciation, assigning similar values to phonetically alike words. This algorithm generates an alpha-numeric code wherein first character is an English alphabet followed by some numbers. First alphabet is usually the first alphabet of the given string and other numerals depict the next sounds of the string.

For example, the soundex codes for 'Geeta', 'Gita' or 'Geetha' are same which is G300.

On the other hand, the soundex code for ‘geetagovindam’ is G321 which is different from earlier generated code.

It can thus be noted that this algorithm may be helpful in detecting similar sounding words in English Language. Detecting distance metric between two strings using this method will however, a challenge.

Metaphone:

Developed in 1990 by Lawrence Philips, Metaphone is a more accurate alternative to Soundex. It considers groups of letters, enhancing its performance compared to traditional phonetic algorithms, i.e. it generates a code for each string, but the code is all alphabets unlike Soundex.

Metaphone codes, for example, would be same ‘JT’ for both ‘Geeta’ and ‘Gita’ but this would be ‘JTKFNTM’ for ‘Geeta Govindam’

Double Metaphone:

Building on Metaphone, Philips extended the algorithm to Double Metaphone algorithm returning two codes and thus, providing more opportunities for matches. However, this increased flexibility comes with a higher probability of errors.

Finding double metaphone codes for both ‘Geeta’ and ‘Gita’ would result in ‘JT’ and ‘KT’ as primary and secondary codes. The codes for ‘GeetaGovindam’ would be however, ‘JTKFNTM’ and ‘KTKFNTM’ respectively.

Metaphone 3:

Philips further refined the Double Metaphone algorithm into Metaphone 3, offering improved results. Notably, Metaphone 3 is proprietary and not open-source.

In navigating the landscape of string matching, understanding the nuances of lexical and phonetic algorithms proves instrumental. These algorithms, with their strengths and weaknesses, empower various applications from data cleaning to record linkage and beyond.

To sum it up, in today's digital age, keeping our sensitive information safe is crucial. As technology advances, we need strong tools, like analytics algorithms, to act as guards for our digital fortress. These tools, especially good at matching names and other text, play a key role in protecting our data. Think of it like this: in the toolkit, there's something called text or string matching. It's a bit tricky when it comes to matching people's names because the way names are spelled can be a personal choice. For example, both 'Rajendra' and 'Rajender' can be right.

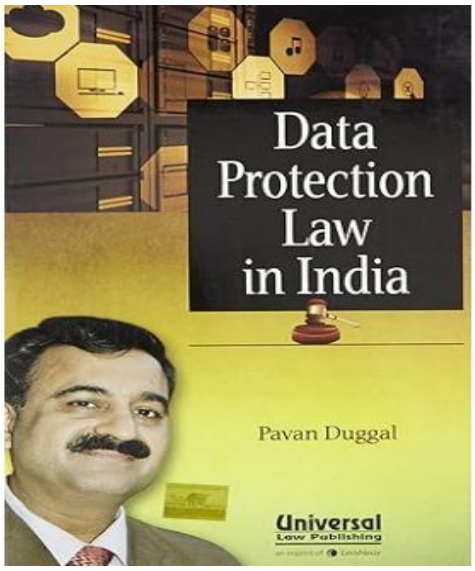
But why does this matter a lot? Especially in audits, where we check financial records and ensure compliance of rules, matching names

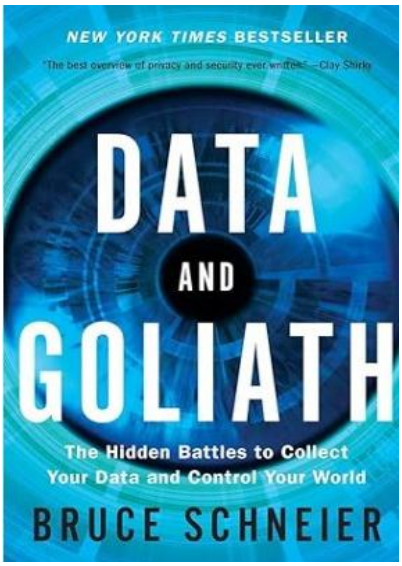
gains paramount importance. It can ensure everything is accurate and may help us in detecting fraud. So, as our digital world keeps changing, these matching tools not only keep our digital fortresses strong but also make sure our important information stays safe from new challenges.

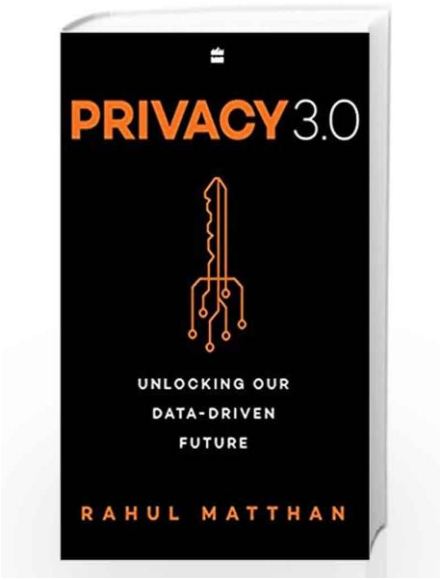
References:

[1] https://bradandkathy.com/genealogy/overviewofsoundex.php
[1] http://aspell.net/metaphone/metaphone.basic
[1] https://github.com/gitpan/Text-DoubleMetaphone/blob/master/double_metaphone.c
[1] http://amorphics.com/metaphone3.html

Suggested Readings on the Topic







Important Links:

- *DATA PRIVACY, ETHICS AND PROTECTION GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA*
- *Managing Digital Risks Primer-ASIAN DEVELOPMENT BANK- December 2023-Asian Development Bank*
- *COMPENDIUM OF DATA PROTECTION AND PRIVACY POLICIES AND OTHER RELATED GUIDANCE WITHIN THE UNITED NATIONS ORGANIZATION AND OTHER SELECTED BODIES OF THE INTERNATIONAL COMMUNITY November 2021*

Quiz

Digital Personal Data Protection

Multiple Choice Questions

Q. 1. Right to Privacy comes under which article of the Constitution of India?

a) Article 18
b) Article 19
c) Article 20
d) Article 21

Q. 2. under which Part of the Constitution of India Right to Privacy comes?

a) Part I
b) Part II
c) Part III
d) Part IV

Q. 3. What is primary objective of the Digital Personal Data Protection Act, 2023?

a) To promote e-Commerce
b) To protect citizen's personal data
c) To regulate online transactions
d) To censor online content

Q. 4. According to Digital Personal Data Protection Act, 2023, Child means an individual who has not completed the age of?

a) 12 years
b) 14 years
c) 16 years
d) 18 years

Q. 5. X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act (Digital Personal Data Protection Act, 2023) shall

a) Apply
b) not apply

Q. 6. A Data Fiduciary shall not, upon receiving a request for correction, completion or updating from a Data Principal, —

a) correct the inaccurate or misleading personal data
b) complete the incomplete personal data
c) update the personal data
d) none of the above

Q. 7. Every appeal under sub-section (1) shall be filed within a period of _____ days from the date of receipt of the order or direction appealed against and it shall be in such form and manner?

a) 180
b) Thirty
c) Forty-five
d) Sixty

Q. 8. What is the timeframe for reporting a data breach under the Act?

a) Within 24 hours
b) Within 72 hours
c) Within 1 week
d) Within 1 month

Q. 9. What is considered sensitive personal data under the Digital Data Protection Act?

a) Name and address
b) Financial information
c) Medical history
d) All of the above

Q. 10. Which personal data can be processed without consent?

a) Sensitive personal data
b) Non-sensitive personal data
c) Publicly available data
d) Data for research purposes

Q. 11. Which act is mentioned as India's first data protection act?

a) IT Act 2000
b) Digital India Act
c) Digital Personal Data Protection (DPDP) Act, 2023
d) National e-Governance Plan

Q. 12. Digital Personal Data Protection Act, 2023 came into effect on?

a) 11 July 2023
b) 11 August 2023
c) 11 September 2023
d) 11 October 2023

Q. 13. What security measure protects data against unauthorized access?

a) Encryption
b) Pseudonymization
c) Access controls
d) All of the above

Q. 14. Digital India Initiative was launched in the year?

a) 2014
b) 2015
c) 2016
d) 2017

Answers:

1	**2**	**3**	**4**	**5**	**6**	**7**
d	c	b	d	b	d	d
8	**9**	**10**	**11**	**12**	**13**	**14**
b	d	c	c	b	d	b

2024 edition