DSCI
PROMOTING DATA PROTECTION

DSCI Digest

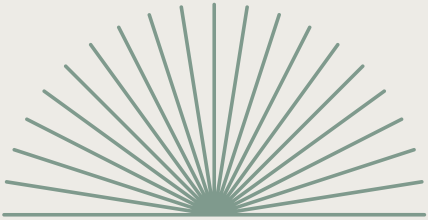
May 2024

DSCI Digest

The DSCI Digest is brought to you for a peripheral understanding of the industry-relevant studies conducted by DSCI. It aims to help you learn and understand the subjects in discussion in a succinct composition.

Table of Contents

- The Future of Data Protection in India: A Roadmap for Regulators 4
- Exploratory Note on Deepfakes and Policy Considerations 7
- Accelerating Public Service Delivery through Cloud Adoption: Revisiting Concerns of Security and Sovereignty 9
- Aerial Insights: The Role of Drone Forensics in Modern Investigations 12



The Future of Data Protection in India

A roadmap for regulators

At the heart of all data generation is the concern of its protection. Afterall, in the era of increased connectivity and dependence on digital/ virtual communication, the apprehension is legitimate. In August 2023, Digital Personal Data Protection (DPDP) Bill was introduced and passed before the Parliament with the intention to provide for the processing of digital personal data in a manner that recognizes the right of individuals to protect their personal data, the need to process personal data for lawful purposes and for other incidental purposes. The bill is now the DPDP Act, a first in terms of a regularized framework for data protection in the country.

Sectoral regulators in the country have also released guidelines and advisories related to personal data protection to ensure organizational compliance with best practices for managing personal data, and have adequate safeguards to prevent unauthorized access, use, or disclosure. The purpose of this report, however, is to identify and examine the potential concerns arising from the DPDP Act.

The report primarily focuses on the following thematic concerns that can be worked upon to refine and improve the DPDPA to have a more robust and effective framework for Data Protection in India. The concern areas include:
Data Breaches, Consent Managers, Cross-border Data Transfers and Data Anonymization.

Data Breaches

The DPDPA 2023, defines a personal data breach as, “any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.”

Both personal data breaches and unauthorized processing can have serious consequences for data subjects and data fiduciaries.

However, with its broad and all-encompassing definition, the DPDPA framework overlooks the distinction between 'unauthorized processing' and breaches of personal data. To resolve the surrounding vagueness, the report recommends for the concepts to be treated separately in implementation and adjudicatory proceedings under the law. The report suggests a risk-based approach to report the data breach where data fiduciaries report in compliance with data protection laws of different jurisdictions. It also suggests the breach reporting should occur in a phased manner to ease the reporting burden on data fiduciaries who can provide information in stages instead of providing complete information at the time of the breach.

Consent Managers

Earlier versions of data protection law in India first laid down the concept of consent management which envisaged a user-centric model for obtaining consent. The objective was to ensure separation of consent flow and data flow. The DPDPA furthers this notion by establishing the concept of 'Consent Managers (CM)' to address the need. Section 2(g) of the DPDPA defines the term 'Consent Managers' as a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Although the Act describes their functions, establishes their scope and stipulates their accountability to the Data Principal. Several ambiguities arise here in terms of the implementation model that the Act envisages for CMs. Primarily, the accountability, technical architecture, and cross-functionality of CMs with existing initiatives may be challenging to navigate.

Therefore, the report recommends that CMs as a technical intervention should not become a mandate. Moreover, clarity on the scope and functioning of CMs should be meted out to recognize them as distinct legal entities and not merely categorize them as "persons". A relook and revision needs to come with respect to the existing industry practices around consent management and operational guardrails concerning consent managers should be prescribed for better functioning.

Cross-border Data Transfers

Under the DPDPA 2023, Section I6 recognizes the significance of cross-border data transfers in promoting global trade and services, and grants the Central Government the authority to notify specific countries or territories outside India to which a data fiduciary cannot transfer personal data. In every industry, be it manufacturing, services, agriculture, or retail, data is a fundamental resource, and its seamless global circulation is vital.

The Act seeks to set up a framework to

facilitate cross-border data transfers. It is, however, important to highlight that the Act lacks clarity and the specificities of notifying restricted jurisdictions and the process for the same will only be outlined in the future through delegated legislation. Therefore, the report recommends enhancing regulatory clarity and certainty for the transfers. Along with a risk-based approach to be undertaken by the data fiduciaries who conduct a comprehensive assessment to identify potential risks and vulnerabilities.

Data Anonymization

The newly enacted Digital Personal Data Protection Act ('DPDPA') 2023 does not refer to anonymized data, even though it has been touched upon briefly in secondary sectoral policies.

However, anonymization is a privacy preserving mechanism for data minimization, risk management and data protection in the cases of unauthorized access. It removes personally identifiable attributes from personal data reducing or eliminating identifiability. Since the rise of hyperconnectivity has limited the ability of organizations and individuals to protect their data.

Given the intensity and scale of data collection, it is not always possible for individuals to exercise control over their personal data in a way that meets the privacy expectations of the data subject or for the data fiduciaries to exercise legitimate objectives of processing simultaneously.

Anonymization, when carried out effectively, is marked by (a) irreversibility, and (b) a strong protection threshold, requiring significant intensive effort to re - identify.

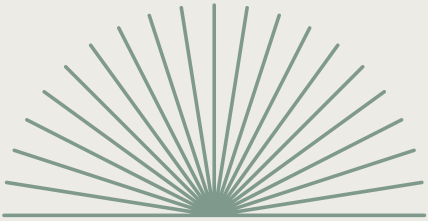
The primitive techniques, such as pseudonymization and data masking, have proven to be the least impressive among anonymization operations due to their vulnerability to easy infiltration. However, the report recommends for usage within organizations with highly secure communication lines for simple analytics or in very specific contexts.

The mentioned aspects are however more detailed as we discuss the associated risks, global approaches and recommendations for the mentioned areas of concern to better the now mandated DPDPA.

To learn more on the subject, visit our report on 'The Future of Data Protection in India Part I & II' where part I focuses on Data Breaches, Consent Managers and Cross-border Data Transfers and part II details on Data Anonymization.

Read more at:
https://www.dsci.in/resource/content/future-data-protection-india





Exploratory note on Deepfakes and Policy Considerations

Deepfake, a word whose echo has created a massive uproar in the present times. While there is no consensus on the precise definition of a 'deepfake', it can generally be understood as synthetic/artificial media which is computer-generated and depicts a scenario which did not actually occur or depicts a person doing or saying something which they did not actually do or say. The term is a portmanteau of 'deep learning' and 'fake'.

The proliferation of deepfake around the world has naturally raised concerns on the policy frameworks to fight off the menace due to its alarming degree of induced harm. Some key areas of concern today are: (i) harms caused to individuals upon distribution of deepfakes without their consent, (ii) data protection concerns, (iii) personality rights and IPR considerations such as determining who owns the content created through deep learning, (iv) proliferation of deepfakes which contain non-consensual sexual content or when such content affects public order, and finally (v) creation of guardrails around development of such AI technology and due diligence requirements pertaining to dissemination and distribution of such content.

Legal frameworks are being revised and proposed across nations to tackle with the issue of artificial media. But concretization is still afar. To elucidate, United Kingdom has the 'Online Safety Act' in place where it tackles deep fakes in the nature of non-consensual intimate images or film. It is a criminal offence to share such deepfakes while the creation of such deepfakes is not regulated. The proposed regulatory focus or legal remedy is 2 years of imprisonment on sharing of deepfake pornography.

The permeation of this form of artificial

media is, therefore, a challenge for policy makers around the world.

Keeping the nation-specific regulations aside, it also becomes important to have industry interventions and technological solutions for addressing the deepfake anxiety.

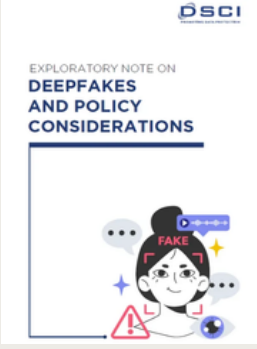
The industry-led Content Authenticity Initiative has proposed a content attribution solution wherein attribution information about a piece of content is cryptographically sealed and verifiable by an individual or organization from creation to consumption. The Coalition for Content Provenance and Authentication has also released an open standard, technical specification for digital provenance. The underlying idea is to make available data about content, where it was created, how and when it has been altered, and who has altered it, in an effort to provide indicators of authenticity.

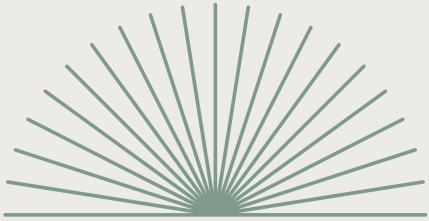
Furthermore, Meta has recently announced Stable Signature, an invisible watermarking technique to distinguish when an image is created by an open source generative AI model. Invisible watermarking incorporates information into digital content. The watermark is invisible to the naked eye. But can be detected by algorithms—even if people edit the images. YouTube has also announced that it will require creators to disclose when they have created synthetic media content that is realistic, including using AI tools. Once rolled out, failure to adhere to these requirements consistently might lead to penalties such as content takedown or suspension from the YouTube Partner Program.

However, there are regulatory concerns such as the legal recourse available to individual victims can be convoluted as it may not be possible to identify the person who has created the deepfake, when such persons operate anonymously. At the core of this issue lies the issue of attribution. The metadata which is required for ascertaining a deep fake's provenance might be insufficient to identify the person who generated it.

There's more to these industry interventions and regulatory concerns, described in detail in our 'Exploratory Note on Deepfakes and Policy Considerations.'

To learn more on the subject of deepfake, visit: https://www.dsci.in/resource/content/exploratory-note-deepfakes-and-policy-considerations





Accelerating Public Service Delivery through Cloud Adoption

Revisiting Concerns of Security and Sovereignty

India is swiftly advancing in digitization, with virtually every aspect of our lives now digital. This remarkable progress stems from a revolution in the production and consumption of digital resources in various forms. The rapid shift from the physical realm to the virtual world has prompted governments worldwide to adapt public service delivery to a wider audience. To achieve this, they are increasingly utilizing cloud computing solutions to improve e-governance and service delivery. As per the National Institute of Standards and Technology (NIST) definition cloud computing is, "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." The NIST report was an early intervention to provide a baseline for discussion on what is cloud computing.

However, due to its technicality, the definition may pose ambiguity for the reader. Hence, there may be questions such as whether a computer connected to a server over the internet is cloud, or whether on-premises servers are cloud, or whether webpages on the internet are cloud, and whether cloud computing is limited to storage alone.

To regard the cloud as a monolithic technology disregards the many innovations that make the cloud truly universal and convenient. Cloud infrastructure is not limited to the servers and the internet. Each of the servers in a data center has hardware and software sourced from different vendors to manage computing power, division of operations, storage of data, and run external software. Each data center is designed to ensure resilience against failure, connectivity, power outages, and cybersecurity attacks. These technologies that empower clouds must make it an on-demand service so that consumers can utilize computing capabilities without human interaction over their networks and devices.

The biggest boon with these solutions is that they offer enhanced scalability, elasticity, cost-efficiency, security, innovation, and collaboration. Organizations need not build infrastructure for seasonal or irregular spikes for resource demand.

With a select number of global data centers connected via the internet users can provide computing resources from the Cloud Service Providers (CSP) from anywhere in the world according to their demand. The shared infrastructure of the public cloud allows for cost efficiencies since organizations are not tied down to the infrastructure and pay for computing resources they procure as they use. This trend is epitomized by the "Cloud First" strategy, which India, like many others, is also adopting significantly.

The NIST 800-I45 Report also outlines a classification for cloud service models which include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Where IaaS enables consumers to provision computing resources from the cloud provider; PaaS allows the deployment of applications on the cloud infrastructure provided by the provider; and SaaS permits consumers to use applications running on the cloud infrastructure.

Additional classifications exist within ISO standards, such as Communications as a Service (CaaS), Compute as a Service (CompaaS), and Network as a Service (NaaS). However, these are regarded as marketing terms by NIST, not formal service models.

Cloud deployments often combine these service models, and they may not always align neatly with one specific model. The ownership and operation of underlying cloud infrastructure can vary, leading to layered or unlayered deployments. For example, Netflix, a SaaS application, runs on AWS IaaS, while Dropbox, also SaaS, operates on its own infrastructure. This layering concept extends to PaaS applications and can involve deployment on different infrastructure layers provided by third-party providers or consumers themselves.

Despite these provisions and acknowledged advantages of cloud computing solutions, their full adoption for e-service delivery remains hindered by apprehensions regarding national security, privacy, and the relinquishing of data control inherent in cloud storage. These concerns, encapsulated by the abstract notion of "data sovereignty," highlight the jurisdictional implications of data storage, subjecting it to the laws of the country where it resides. Consequently, data sovereignty, often fused with data residency and storage, presents challenges for both governmental adoption of cloud services to enhance public service delivery and for cloud service providers aiming to operate within India.

Hence, it is crucial to tackle the ongoing apprehensions regarding data control, ownership, and security within the cloud, given the significant scale of migration required and the value proposition offered by a cloud computing solution. Moreover, the prominence of the concept of data residency underlines the urgent requirement for an approach that guarantees transparency, privacy, and security assurances across all fronts to enhance data management practices in the cloud.

CSPs are acknowledging these concerns. They are also leveraging technological advancements and innovations, and are granting users comprehensive control over their data within the cloud. This shift prompts a reassessment of the conventional significance of data residency in cloud environments, aiming to cultivate a balanced synergy between the innovative possibilities of public cloud adoption and the necessity to maintain control over stored data.

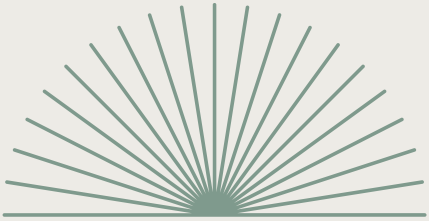
A thorough reassessment necessitates a deeper comprehension of technology itself, encompassing various types of cloud computing solutions, deployment models, technical specifications, and their mapping against concerns regarding security, privacy, ownership, and control. While acknowledging the current capabilities of CSPs in ensuring superior security compared to on-premise solutions, genuine concerns arise regarding Law Enforcement access to data stored abroad, warranting a delineation of its contours.

Similarly, aligning clients' or government entities' privacy expectations with CSPs' data protection practices is imperative. Assessing the technology employed to ensure ownership and control rests with the client is pivotal, without solely relying on data localization/residency practices. While the intent is to foster innovation, evaluating existing laws to determine whether they facilitate harnessing the full potential of CSPs is crucial for accelerating public service delivery through the public cloud.

Such a comprehensive assessment aids in deciphering the actual issues and formulating actionable recommendations to synergize the anticipated outcomes of recent technological advancements in the context of cloud computing. Intriguing, isn't it? This is precisely the focus of this report, delving deeply to unveil the true potential of public cloud in advancing public service delivery through cloud adoption.

To gather a more comprehensive outlook of the subject, head to the report and read more at: https://www.dsci.in/resource/content/accelerating-public-service-delivery





Aerial Insights: The Role of Drone Forensics in Modern Investigations

"Drones, unmanned aerial vehicles, or UAVs, have become a key component of the rapidly developing technological revolution, transforming industries and improving scientific research. Drones' wide adaptability and accessibility have enabled innovative uses in almost anything from infrastructure inspection and precision farming to wildlife monitoring and disaster relief," says IAS Umashankar SR while drawing our attention to the prowess of drone technology.

Their utility can be seen across a multitude of sectors, including military, rescue operations, agriculture, space exploration, wildlife monitoring, medical services, delivery, photography and more. Their deployment enhances the effectiveness and safety of diverse activities like surveillance, targeted operations, transportation, seeding, mapping, and beyond.

But moving with a revolutionary technology also requires better attention to all the complexities and challenges that come in with the advancement. As continued development raises noteworthy concerns regarding potential risks and ethical considerations. These include issues like invasion of privacy, collisions in airspace, accidents, terror incidents, cyberattacks, and environmental impact.

Crimes involving drones have become more prevalent with their widespread availability and capabilities. Drones equipped with cameras can be used for spying on individuals or private property without consent and violating privacy laws. There are some instances where criminals have used drones to smuggle contraband, including drugs, electronics, or other illegal goods across borders or into restricted areas.

To handle such cases, it becomes important to devise the best possible mechanism to search, seize, acquire, and analyze drones. This would aid investigators/ examiners in the identification of incriminating evidence such as flight-captured photos and videos, flight logs, waypoints, etc. Therefore, gaining insights into the characteristics of different popular drones available in

the market and to develop possible ways for acquiring and analyzing the extracted data from the drones is of prime importance here. The most worrisome aspect to this understanding is that the technology related to drones is on the verge of progressive growth but digital forensics relating to drones is evolving at a slower pace.

Older techniques are becoming obsolete due to the release of new-age drones in the market, offering encryption by default. The drones today offer a variety of hardware specifications, operating system versions, and security features, the data extraction from drones and analysis of extracted data is becoming more complicated day by day. Without dedicated digital forensic solutions, law enforcement officers and forensic examiners face obstacles in identifying perpetrators, flight patterns, and uncovering evidence to support legal proceedings.

But solutions are available. Analysis methods to effectively identify crucial evidence that can either substantiate or refute the illicit activities in question is the need of the hour. To better understand the system of drones it is important to first understand the key components. Physical component comprises of drone body, flight controller, motors and speed controllers, protective casing, GPS receiver, radio receiver, radio transmitter and LED lights.

The software component includes; flight management software and ground control software for controlling the drone flight flight operation and for managing pre-defined navigation routes respectively.

Apart from the constituent components, the drones we see today have diversified categorization.

Categories of Drone

Recreational Drones: The focus for these drones is affordability and outdoor use and are designed for enthusiasts and children alike.

Commercial Drones: These are involved in photography, or land survey, and their classification is based on user intention rather than device capability. Aiming at professionals, these drones come equipped with specialized payloads, such as cameras for professional photography, industrial inspection, or land survey.

Bespoke Drones: These are not pre-assembled and are customized by owners using individual components, allowing for flexibility in design and functionality.

Keeping the physicality and categorization aside, drones can be further sub-divided basis of the their appearance.

Types of Drones

Fixed-wing Drones: These look like airplanes, with a fixed main wing. They typically include a fuselage, wings, propeller, and motor. They require specialized training for control

and are unsuitable for hovering or stationary surveillance.

Single-Rotor Drones: They have a design resembling helicopters, featuring a single large rotor for lift and propulsion, and are capable of versatile maneuvers.

Fixed-Wing Hybrid Drones: These drones are a combination of fixed-wing and multirotor designs. They may have rotating wings or other mechanisms that allow for vertical take-off and landing.

Multirotor Drones: They are commonly known as quadcopters, have multiple rotors arranged in a symmetrical pattern. They can hover, ascend, and descend vertically.

Such wide variety of drones is only to show you the glimpse of how far the technology has come. Therefore, understanding drone forensics and its applications in crime detection is a must. There are several such applications of drone forensics in crime investigation. First, crime prevention and detection where analysis of data retrieved from confiscated or downed drones can reveal valuable information about the operators, their motives, and potential links to criminal networks.

Second, incident reconstruction where scrutinizing the digital footprints left behind by drones can help in reconstructing the events leading up to an incident and aid in the determination of liability along with the formulation of preventive measures.

extract and analyze data, shedding light on the activities of the drone and its operator.

Fourth, regulatory compliance as it will help in verifying whether operators adhere to established guidelines, enabling authorities to take appropriate action against those who violate airspace regulations or engage in unlawful activities.

Fifth, national security to investigate and mitigate security breaches, helps in understanding the technology and tactics employed by malicious drone operators.

The breaches are bound to happen, if judicious use of the suggested applications is done along with the search and seizure of malicious drones a lot of investigative control can thus be gained.

A more exploratory take on this is elaborated for you as law enforcement agencies and forensic examiners to read at: https://www.dsci.in/resource/content/aerial-insights-role-drone-forensics-modern-investigations



What to Expect in the Next Edition

The DSCI Digest offers a condensed version of all our publications, giving you a quick overview to help you decide on your next read.

The subjects catered here enable you to gain first-hand information on the volumes we bring out for the industry. The information shared is a brief account of the conducted studies, you are requested to visit the reports on our website for better understanding.

https://www.dsci.in/knowledge-center/study-and-reports

Authors

- “Accelerating Public Service Delivery through Cloud Adoption” by Deepa Ojha
- “Aerial Insights: The Role of Drone Forensics in Modern Investigations” by Jaya Shankara & Shashidhar T K
- “Exploratory note on Deepfakes and Policy Considerations” by Deepa Ojha & Shivangi Malhotra
- “The Future of Data Protection in India” by Shivangi Malhotra

Compiler and Editor

Mridushi Bose

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by nasscom, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, FOURTH FLOOR, PLOT. NO. 7-10, SECTOR 126, NOIDA, UP - 201303

+91-120-4990253 | INFO@DSCI.IN | WWW.DSCI.IN

dsci.connect dsci.connect dscivideo data-security-council-of-india DSCI_Connect

All Rights Reserved © DSCI 2024