Resources to Help Understand the Data Privacy Laws in India

India is ready to embark upon a journey with the Data Empowerment and Protection Architecture (DEPA), which aims to empower individuals with control over how their personal data is used and shared. There are several important unique requirements of India given the prevailing local realities. The Information Technology Act, 2000 (IT Act), and its Rules, inter alia protect digital Personal Data in India, but have been found to be lacking on multiple counts. A new dimension to protect Personal Data is awaited once the Personal Data Protection Bill, 2019, (PDP Bill) is enacted. Effective implementation of the regulatory, institutional and technology design for securing data sharing will be the key challenge.

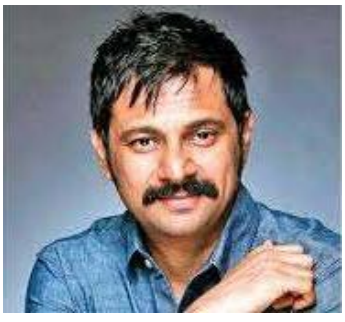
The Authors

Khushbu Jain
Founder & Managing Partner
Ark Legal

Khushbu Jain is a practicing advocate before the Supreme Court of India. Her area of expertise includes litigation practice pertaining to business/ corporate; she also handles matters pertaining to Information Technology, and Crime.

She is a consultant to members of SEBI and advises them on issues ranging from Prohibition of Fraudulent and Unfair Trade Practices (PFUTP), Embezzlement, Prohibition of Insider Trading (PIT) and other relevant issues. She has successfully defended several clients facing cartel and bid-rigging trials and has advised them on numerous Abuse of Dominance matters.

She is also a public speaker, opinion column writer for newspapers. She speaks and writes extensively on issues related to corporate Law, Privacy, and cyber issues.



Brijesh Singh
Inspector General of Police
Government of Maharashtra

Mr. Singh is an elite Indian Police Service officer with prior stint as special inspector general of police with the CID and also headed the cybersecurity department of Maharashtra State. He successfully implemented Crime Criminal Tracking and Networking Systems (CCTNS) project in Maharashtra State. Due to his efforts, Maharashtra implemented path-breaking IT schemes like online first information reports (FIRs), advanced forensics, and digitization of the state's crime records. Singh is also the designated Special Inspector General of Police - Women Atrocity Prevention, a special authority created by the Maharashtra government.

Mr. Singh has also been designing apps for mobile platforms and holds several patents. He constantly contributes to the evolving software innovation space, and is the author of "Quantum Siege," which is among the top ten books on online ecommerce portal, Amazon.

DEPA: The Technology of Consent, India Style

The Data Empowerment & Protection Architecture aims to empower individuals with control over how their personal data is used and shared. If successful, it will ensure the economic inclusion of the underprivileged, a substantial reduction in banking frauds, and the creation of business opportunities for many smaller players.

"In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition." — Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe, about privacy.

In the beautiful tech-savvy Baltic nation of Estonia, whenever any authority accesses the data of a citizen, the person is duly notified about the event and the reasons for such access. The Estonian government has no central servers or a master database; instead, each agency or organisation stores and administers its own data in encrypted form, and it cannot be shared without the knowledge and permission of the subject. Thus, data about any citizen's taxes, traffic challans, land transfers, education, voter registration, healthcare and finances are stored in separate databases. One can choose which service providers see information from other providers — so, for instance, the data subject decides if he/she wants the family physician to see information from the psychotherapist or cardiologist or the skin doctor.

India is ready to embark upon a similar journey with the Data Empowerment and Protection Architecture (DEPA). This will be achieved by implementing regulatory, institutional and technology design for secure data sharing. According to NITI Aayog, "The Data Empowerment & Protection Architecture will empower individuals with control over how their personal data is used & shared while ensuring that privacy considerations are addressed."

DATA, PRIVACY, SECURITY & INNOVATION

A new class of institutions will be created that have economic incentives aligned with those of the users with regard to the sharing of personal data. Consent managers — organisations maintaining the 'electronic consent dashboard' for users as stipulated in the PDPR Bill — will mediate the interaction between an individual, a potential data user, and the data fiduciary holding a user's information. Consent managers will be in the business of making sure that individual data is not shared without user consent and that individual data rights around privacy and portability are protected. The DEPA framework envisions these consent managers as 'data blind' entities that will not see or use personal data themselves and instead serve as a conduit for encrypted data flows. They are not permitted to store user data either.

As the DEPA evolves, other technology modules would be added which would be more efficient at preserving privacy and data rights, and both public and private players will be allowed to contribute to this.

DATA BARONS AND ENTRY BARRIERS

Big Tech firms with access to very large amounts of data use that data to improve the quality of their products and services. This is done by increasing the accuracy of a search engine, improving targeted advertising or offering targeted discounts: a process which attracts additional customers, who in turn generate more data. This also creates the phenomenon of 'network effects' which amplify the existing advantage of one amassing data. Similarly, the access to big data results in a feedback loop which reinforces the dominance of large firms.

Thus, the customer or user cannot 'multihome' or use portability to his/her advantage, getting into a provider/vendor lockdown. DEPA has the potential to break this cycle by unlocking data in institutional silos. This will provide significant opportunities for a number of players, including banks, financial institutions and gaming

operators, to redefine their business and operating models to generate new value propositions and provide innovative customer solutions. DEPA promises to open up consumer bank accounts to third-party providers, thereby, unlocking banks' data-lakes and providing a level playing field with other financial services providers.

There are four recognised criteria for being a barrier to entry — inimitability, rarity, value, and non-substitutability. Large technology corporations hoarding data to their own advantage do not fulfil any of the above. While participating in the deliberations on non-personal data, the authors of this article have strongly advocated the need to break these entry barriers down and look at data as commons.

OPEN BANKING AND SHARING WITH CONSENT

Legislation can hinder innovation if it is technically restrictive or impacts the speed of technological progress, and an uncertain regulatory space may create an atmosphere of risk for investments. There is a need to achieve an optimal balance between the predictability of the regulatory environment and adaptability to technological and scientific progress.

Rather than letting the private sector drive the technology, the Indian government has sought to impose standards, and even cooperation, through regulations, technological architecture, and frameworks. The "Indian way" to digital empowerment intends to create a transformative platform that exhibits an entirely novel approach on data protection, sharing, consent and privacy.

DEPA AND THE ORGANS PRINCIPLES

DEPA democratises access and enables secure portability of trusted data between different service providers. It involves the creation of a standardised technology architecture implemented within the right institutional constructs.

DEPA's technology architecture is an interoperable, secure, and privacy-preserving framework for data sharing through:

1. A technology standard for a machine-readable consent artefact; and
2. Open APIs for data sharing; and
3. A standard for financial information.

Consent under DEPA will adhere to the ORGANS principles, that is:

1. Open standards: the approach needs to be interoperable across institutions
2. Revocable: individuals must be able to revoke consent
3. Granular: consent must be provided each time, should stipulate for how long certain data is accessed, etc.
4. Auditable: machine-readable logs of consent should be provided
5. Notice: must be provided to all parties
6. Secure by design

DEPA FEATURES AND ADVANTAGES

This will develop a novel consented data-sharing architecture to accomplish these goals. Findings so far have shown that, in current day applications, consent is handled very loosely and, oftentimes, insecurely.

DEPA has the following features which ensure that there is a practical means to access, control and selectively share personal data stored across multiple institutional datasets:

A. Electronic Data Consent (EDC): Guiding principles for the sharing of user data across different services with user consent have been outlined previously in two key policy documents, namely, the "Policy on Open Application Programming Interfaces (APIs) for the Government of India", published by the Ministry of Electronics and Information Technology (MeitY), and the "National Data Sharing and Accessibility Policy (NDSAP) 2012" by the Department of Science & Technology. Electronic consent allows for data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability to ensure that the data trails can be audited in the future.

B. Technology tools for consented data sharing: The Indian government is envisaging a comprehensive technology framework to enable the effective and secure implementation of DEPA. The technology framework should be open, secure, user-centric and application-agnostic. Using electronic consent, rather than requiring users to share credentials like passwords or to sign paper documents, transactions can be done and services rendered. With this framework, data consumers (like government departments, employers, lenders, etc) can securely access data of users from providers (like government departments, banks, etc.)

C. Consent management system: DEPA's institutional architecture involves the creation of new market players known as consent managers who play the role of enabling consent management for the user. These consent managers are 'data blind' and will not see user data themselves, rather they will serve as a conduit for encrypted data flows.

D. Individual-centric approach: The individual-centric approach of DEPA encourages user control on data sharing for empowerment. By giving people the power to decide how their data can be used, DEPA enables an individual to control the flow of and benefit from the value of her personal data, relying on not only institutional data protection measures, but also restoring individual agency over data use.

E. Promotes user control on data sharing for empowerment: The objective of DEPA is to provide the tools and utilities that enable us to build systems that can provide the user with the mechanisms for protecting and sharing their data. It is imperative to engender a trusted mechanism for the sharing of data by giving the people control of their data. DEPA opens whole new models for privacy protection and auditing data flows while keeping the user at the centre.

ISSUES AT THIS POINT

In 2015, the European Union acted to create a 'digital single market' for payment services in Europe, which is similar to what India is attempting. The EU's Second Payment Services Directive (PSD2) strengthened consumer rights, introduced new security measures, and provided the regulatory infrastructure for its own form of Open Banking ('OB'). DEPA is principally trying to achieve comparable objectives.

A study by the global consulting firm Roland Berger, "Adapt or die? Why PSD2 has so far failed to unlock the potential of Open Banking", finds: "In the implementation of PSD2, there is still a wide gap between ambition and reality. The established financial service providers have limited themselves primarily to meeting regulatory requirements." Banks in the EU had a deadline until March 2019 to establish a "sandboxed" environment that third-party providers could access and use to test products. However, according to open banking platform Tink, 41% of the 442 European banks surveyed failed to meet the deadline.

Learning from the EU experience, driving changes in technology infrastructure at this scale may not be easy, and consumer awareness and stakeholder change management will also be crucial factors in its success or failure.

CONCLUSION

The world has seen the Silicon Valley model of innovation where almost everything operates on the principle of least interference and minimal regulation, thus driving immense economic benefits. India has however embarked upon a path of creating regulation led innovation through 'India Stack' in the delivery of public services. It is a set of APIs that allows government, businesses, start-ups and developers to use India's digital infrastructure to deliver private services. These include Aadhaar, Aadhaar-based eKYC, Aadhaar-based eSign for digital contracts, UPI, DigiLocker, etc., and the Open Credit Enablement Network (OCEN) for lending.

What DEPA aims for, in this context, is to put back citizens at the helm of their affairs. They decide what data they want to share, with whom and for what purposes. The proposed architecture ensures privacy and spurs innovation at the same time, unlocking the economic value of data locked up in institutional silos. It is a bold step which, if successful, will ensure the economic inclusion of the underprivileged, a substantial reduction in banking frauds and cybercrime as well as the creation of business opportunities for a large number of smaller players who are disadvantaged in the current scheme of things.

Article: https://thedailyguardian.com/depa-the-technology-of-consent-india-style/

Data is "Inflammable" Oil

The year 2019 was the worst in the history of data breaches. More than 5,500 large breaches resulted in approximately 8 billion leaked records. Most affected sectors were health, followed by financial, energy, industrial and pharma. Even the Education sector was badly hit. A worrisome factor of these breaches and hacks is that the average time to discover a breach is more than 200 days (IBM study). As this article was being written, news came that in May 2020 8.8 billion records had been breached, exceeding the volume of the entire last year. The effects and potential harms of a data breach are multifarious.

Apart from a breach of privacy and loss of money to the customers, data breaches result in loss of business to the corporates. The biggest breaches in numbers included 275 million records of Indian job seekers, Microsoft's 250 million customer records, phone numbers of 419 million Facebook accounts that were leaked, 139 million users of the graphic design service Canva. Another disturbing trend is the increasing cost of the average data breach. The IBM's latest annual Cost of a Data Breach study pitches it to $3.92 million per breach. These costs include notification costs, forensics and investigation, damage control, repairs, lawsuits as well as regulatory fines and other administrative costs.

The legal obligations to secure personal information include an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 requires businesses to use "reasonable security procedures and practices to protect personal information from unauthorised access, destruction, use, modification, or disclosure. The organisations should adopt security standards to achieve an appropriate standard of care for personal information. Some practices Indian corporates can adapt are:

TIMING PROVISIONS

There should be timing provision, which allows for achieving an appropriate balance with a specific deadline intended to prevent major delay, the outer bound may become the de facto standard for notification. The time

needed from discovery to notification with specific industry as a deadline of 30 or 45 days would be too long in many industries and might be too short in others. This provision of timeframe must also be in tune and updated as what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to quickly provide consumers with remedies.

BREACH NOTICES

Easier the better. Such breach notices shall be easier to understand by using/ restricting to a format that will make them easier to understand by prescribing one of two options: (i) use the title "Notice of Data Breach" and the headers "What Happened", "What Information Was Involved", "What We Are Doing", What You Can Do", and "For More Information;" or (ii) use the form provided in the statute. There can be a provision for mandating the companies to post such breach notice on their website after.

How do breaches occur?

1. **System vulnerabilities:** Cybercriminals are constantly looking to exploit and when most software companies are updating their products to keep up with advancements in hardware capabilities, some of these updates create unexpected vulnerabilities. At times, it is not the software upgrade that is vulnerable but thirdparty vendors that may have access to your system are not secure. One such example: the Target data breach (one of the largest data breaches in history).

2. **Weak passwords:** Using passwords such as 'password' or '123456' which tops the list of most commonly used passwords in the last decade. Or the extreme of using most complicated passwords and frequent password changes which forces employees to write and often store in unsecure or predictable locations. Reusing passwords which makes it easier for hackers to target sites with minimal security, helping them to break into sites with much higher security.

1. **Employee negligence:** Employee negligence is number one cause of all security breaches. One of the prime reasons for a ransomware attack is the result of a phishing or social engineering attack aimed at tricking employees into clicking on a malicious link.

Advisory

1. **Limit access:** Restrict providing any one employee access to all systems. Provide access only to those systems and the specific information that are necessary in respect to their jobs. Also, make sure you disable and purge old user accounts. Disable user accounts after employee's exit.

2. **Back up important data:** Back up important data on each computer used in your business. It is necessary to back up this data because computers die, hard disks fail, employees make mistakes, and malicious programs can destroy data on your computers. Test your backups to ensure they can be read on regular intervals.

3. **Securely dispose of stored data:** When disposing of old computers containing sensitive information, business, or personal data, make sure the same is cleaned and disposed of securely.

4. **Unique accounts:** Each of your employees should have an individual account with a unique username and password. Without individual accounts for each user, you may find it difficult to hold anyone accountable for data loss or unauthorised data manipulation.

CONCLUSIONS

Data breaches are here to stay; corporates should evolve a strategy of risk governance rather than risk avoidance. This entails changes in the way we acquire, process, retain and dispose of data. With the advent of a data protection legislation in India, it would be incumbent upon anyone dealing with data of personal nature to take stringent measures with a view to protect individual privacy, dignity, and other legitimate interests.

Cyber security has been gaining ascendance as a critical business consideration, and today it has become existential. Corporates and governments need to understand that there is a huge cost-benefit asymmetry in cyberspace, which needs to be addressed as of yesterday. This would entail huge investments in encryption, anomaly detection, threat hunting, hardening of critical infrastructure, collaboration, and threat intelligence sharing. A comprehensive understanding of what one is protecting and how it can be attacked is essential to build the right data protection posture.

Data today is not limited to its economic value; it has myriad dimensions ranging from strategic to aspects of statecraft. Data is the new oil, more inflammable than the other; it is time to get the act right or risk losing reputation, trust, business and even sovereignty.

Brijesh Singh is an author and a senior IPS officer. Khushbu Jain is a practising advocate before the Supreme Court and founding partner, Ark Legal.

Article: https://infinix.dailyhunt.in/news/india/english/the+daily+guardian-epaper-thdygre/data+is+inflammable+oil-newsid-n197337786?pgs=N&pgn=0&

Why can't I delete my nudes? A Case for Right to be Forgotten

Granting citizens across the globe the 'right to be forgotten' can be a welcome move in the Internet age but legislating on it will require striking a fine balance between matters of privacy, censorship, freedom of expression and corporate policies.

Technology has fundamentally changed our lives, but it has also created inexorable and unanticipated societal repercussions. The fundamental principles inherent in our Constitution and the Indian legal system have faced the challenge of harmonising discordant facets and the impacts of such developments. The Right to Privacy was declared an integral part of the Right to Life and Personal Liberty (Article 21 of the Constitution) vide K. Puttaswamy Judgement by the apex court. Whether to consider the 'Right to be Forgotten' as part of the Right to Privacy is a conundrum which courts around the world, including the Indian judiciary, are being forced to consider or opine upon. The cause célèbre encompassing the Right to be Forgotten is the intersection of the Right to Freedom of Speech and Expression and Right to Privacy.

Processing certain personal data is permitted when the controller's legitimate interest requires it. The controller's economic interests are not enough to overcome the interference with the data subject's privacy rights. The process to strike a balance between full access to uncensored information versus protecting a person's image and well-being by allowing post-hoc censorship of information detrimental to that person has to be fact intensive.

CLASH OF RIGHTS IN THE DIGITAL SPACE

Counterbalancing conflicting fundamental rights in a contested digital space is a tightrope walk. The very jurisprudence of digital human rights is in a nebulous state where the boundaries of these individual rights coalesce and clash, making any estimation or evaluation fraught with polemics. For instance, consider the case concerning a

Spanish citizen's request to have personal information delisted from internet search engines. The Court of Justice of the European Union (CJEU) on 13 May 2014 passed a judgement which firmly established the "right to be forgotten" and also affirmed the idea that personal data should not be indefinitely stored in databases. But this ruling has had very divergent reactions. Significantly, this ruling went against the June 2013 opinion of Advocate General Jääskinen, who felt that the establishment of the "right to be forgotten" in the European Union would leave the bulk of the decision on fundamental rights down to search engines. He also opined that RTBF would curtail the right of expression of the original publisher of the said content. France's data protection authority subsequently ordered Google to extend its removal of links to any Google site globally (not just limited to the EU). Google resisted this initially, refusing to comply with the French order on the ground that "no one country should have the authority to control what content someone in a second country can access".

These judgments and orders were portrayed in the media as a battle between the right to privacy and the freedom of speech and created widespread concerns regarding censorship in the garb of individual privacy. The US and European approach to the primacy of individual freedoms and rights are fundamentally different. While the US gives utmost importance to the freedom of speech and expression, even refraining from limiting hate speech at times, Europe culturally values privacy more than FOE. A future legal conflict would involve an asserted First Amendment right of free speech versus a statutory or common law right to be forgotten. In this scenario, the freedom of speech may start out with an edge, being an established constitutional right. Constitutional rights, however, are not absolute and subject to reasonable restrictions. Even in case of a conflict between two constitutional rights, there is still a need to decide how to resolve the conflict, and future constitutional law developments will be an interesting space to watch.

INFORMATIONAL SELF-DETERMINATION

Privacy is an elusive concept which is difficult to define precisely. Generally, what we mean by privacy is a desire that our personal information be left alone and not interfered with. RTBF is actually a claim for control over our personal information. It is entirely up to individuals to decide how much of their private sphere they decide to share with others.

The notion of informational autonomy naturally finds application to the regulation of online privacy: both the EU and Strasbourg Courts have recognised it as a key value underlying both data protection and Article 8 ECHR. Recital 7 of the GDPR states that, "natural persons should have control of their own personal data"; the Strasbourg Court in one ruling opined that Article 8 ECHR, the right to privacy, "provides for the right to a form of 'informational self-determination'.

It is true that the information available on the internet has been shared by individuals themselves in the first place, which is why some argue that people "invade their own privacy". However, even in this culture of internet exhibitionism and voyeurism, it is only when someone's control over their private sphere is taken from them that their privacy is invaded. Thus, the important postulate here is that, while the boundaries between self-expression and privacy will always vary between people, it in no way means that individuals should be deemed to have given up the core right to privacy.

REVENGE PORN & RIGHT TO BE FORGOTTEN

Justice S.K. Panigrahi of the Orissa High Court recently observed that "allowing videos/photos of rape victims to remain on social media is violative of their fundamental right to privacy," and also that "it is their (victims') right to enforce the right to be forgotten as a right in rem".

Several lawsuits and significant media attention surrounding revenge pornography have facilitated a transformation to the traditional philosophy which says that web searches should reflect the web in its entirety. The revenge pornography epidemic entails mostly vindictive postings on the internet of nude pictures by an "ex" without the other's consent.

Google and other search engines have amended their policies to safeguard the rights of victims. This decision was made weighing the utility of public access to revenge pornography against the damage suffered by individual victims of this crime. This change clearly depicts the ability to recognise the intersection between right to privacy and freedom of speech and expression. It also reflects the slow encroachment of big tech into a quasi-judicial domain.

There have been a wide variety of attempts to deal with the deleterious effects of technology, especially regarding minors and women. The first law of its kind for protecting minors online was introduced on 1 January 2015 as the California's Children's Online Privacy Protection Act 2015 or 'CalOPPA'. One of the aspects of CalOPPA was the 'eraser button', which mandates Internet companies to provide a method by which minors can delete a posted picture from a website. It also mandates websites to provide clear instructions to minors as to how they may remove content they have posted online and the website may be required to make certain content invisible to other website users. However, such erasure of content is limited to content posted by the individuals themselves but not content posted by someone else.

POLEMICS AND PREDICAMENT

Implementation of the Right to be Forgotten in practice poses significant problems as it is impractical/ impossible to remove content from the internet effectively because of the ease with which content is duplicated and transferred and stored by data fiduciary and users. De-linking specific websites or images does little to prevent content from reappearing and content usually remains in its original location where people can continue to find it by typing in specific URLs into their browser or visiting that specific website.

Germany's Federal Constitutional Court, the Bundesverfassungsgericht, issued a pair of rulings on 'right to be forgotten' cases, now called RTBF 1 and RTBF 2, where it circumscribed the reach and territorial application of the earlier Google Spain case, observing that "search engines must find a balance between the public's right to information and an individual's ability to live without impairment due to past events". The judgments also clarified the relationship between the fundamental rights of the national constitution (Grundgesetz), the EU Charter of Fundamental Rights and the European Convention on Human Rights.

CONCLUSIONS

A hyper-connected world which makes individuals virtually omnipresent will cause tectonic political, psychological, and social upheavals, unsettling traditional and accepted modes of interaction, interchange, and strife. We are already moving in this direction as we see institutional changes where technology giants are increasingly taking over the functions of a democratic polity and acting as a quasi-judicial authority, adjudicating on questions of privacy, freedom of expression and criminal jurisprudence.

In an arena of conflicting rights, the means and measures for achieving congruence between seemingly incompatible objectives need to be developed with great care. The Right to be Forgotten has various contours which affect human dignity and well-being while overlapping with other fundamental rights. Evolving jurisprudence will have to take into account geographical and territorial application, national sovereignty, media privileges, individual liberties, transparency and accountability among other things.

New technologies will chart untrodden paths with monumental impacts on life, liberty and human dignity. While humanity embarks on this journey, it has to be mindful of basic human values and ensure that technology is only a means to an end—that of achieving human well-being.

Article: https://thedailyguardian.com/why-cant-i-delete-my-nudes%ef%bb%bf-a-case-for-right-to-be-forgotten/