SUPREME COURT JUDGEMENT ON PRIVACY- EFFECT ON BUSINESS

A Study Project submitted to **ICSI-WIRC**, Mumbai, in partial fulfillment of the requirements for **91st Management Skill Orientation Programme (MSOP)** Course in CS

From: Group 2

1. Swapnil Indurkar
2. Riddhi Desai
3. Sherry Jain
4. Mahek Rupwani

Under Guidance:

Mr. Sharad Jhunjhunwala

INDEX

CHAPTER I:

RESEARCH METHODOLOGY

❖ STATEMENT OF PURPOSE

The purpose of this Research Project is to study and understand Judgement on "Right to Privacy' given by the Honourable Supreme Court Judgement and effects of the same on various Businesses which includes both positive and negative effects. This Research Project intends to provide clear insights of the said Judgement and the various implications that resulted in due course of time.

❖ OBJECTIVES OF THE STUDY

1. To understand the meaning and importance of Right to Privacy

2. To understand the Supreme Court Judgement on Right to Privacy

3. To study the effects of Supreme Court Judgement on Right to Privacy specifically on Business.

4. To understand the overall implications of the said Judgement

❖ DATA COLLECTION

As the Research topic is based on a decided Judgement, our Research Methodology was to review and collate the Secondary Data available from various sources and conduct a deep study of the same.

CHAPTER II:

INTRODUCTION

❖ WHAT IS PRIVACY?

According to Black's Law Dictionary *"right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned"* is defined as Privacy.

Privacy is about respecting individuals and their personal life. Internet privacy is a sub- category of data privacy and the same can arise in response to information from a wide range of sources, such as:

- healthcare records,
- criminal justice investigations and proceedings,
- financial institutions and transactions,
- genetic material,
- privacy breaches,
- residence and geographic records,
- user preferences using persistent cookies.

Therefore, internet privacy is not only important but obligatory. It is our mutual responsibility to protect it, with individual and collective awareness and action.

❖ RIGHT TO PRIVACY-THE BASICS

Article 21 of the Constitution of India states that "No person shall be deprived of his life or personal liberty except according to procedure established by law". It has been interpreted that the term 'life' includes all those aspects of life which go to make a man's life meaningful, complete and worth living.

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

The right to privacy in India has developed through a series of decisions over the past 60 years. Over the years, inconsistency from two early judgments created a divergence of opinion on whether the right to privacy is a fundamental right. The judgement by the Honorable Supreme Court reconciles those

different interpretations to unequivocally declare that it is. Moreover, constitutional provisions must be read and interpreted in a manner which would enhance their conformity with international human rights instruments ratified by India. The judgment also concludes that privacy is a necessary condition for the meaningful exercise of other guaranteed freedoms.

❖ CASES THAT CASTED DOUBTS ON THE RIGHT TO PRIVACY

In 2012, Justice K.S. Puttaswamy (Retired) filed a petition in the Supreme Court challenging the constitutionality of Aadhaar on the grounds that it violates the right to privacy. During the hearings, the Central government opposed the classification of privacy as a fundamental right. The government's opposition to the right relied on two early decisions—MP Sharma vs Satish Chandra in 1954, and Kharak Singh vs State of Uttar Pradesh in 1962—which had held that privacy was not a fundamental right.

In M.P Sharma, the bench held that the drafters of the Constitution did not intend to subject the power of search and seizure to a fundamental right of privacy. They argued that the Indian Constitution does not include any language similar to the Fourth Amendment of the US Constitution, and therefore, questioned the existence of a protected right to privacy. The Supreme Court made clear that M.P Sharma did not decide other questions, such as "whether a constitutional right to privacy is protected by other provisions contained in the fundamental rights including among them, the right to life and personal liberty under Article 21."

In Kharak Singh, the decision invalidated a Police Regulation that provided for nightly domiciliary visits, calling them an "unauthorized intrusion into a person's home and a violation of ordered liberty." However, it also upheld other clauses of the Regulation on the ground that the right of privacy was not guaranteed under the Constitution, and hence Article 21 of the Indian Constitution (the right to life and personal liberty) had no application. Justice Subbarao's dissenting opinion clarified that, although the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21.

Over the next 40 years, the interpretation and scope of privacy as a right expanded, and was accepted as being constitutional in subsequent judgments. During the hearings of the Aadhaar challenge, the Attorney-General (AG) representing the Union of India questioned the foundations of the right to privacy. The AG argued that the Constitution's framers never intended to incorporate a right to privacy, and therefore, to read such a right as intrinsic to the right to life and personal liberty

under Article 21, or to the rights to various freedoms (such as the freedom of expression) guaranteed under Article 19, would amount to rewriting the Constitution. The government also pleaded that privacy was "too amorphous" for a precise definition and an elitist concept which should not be elevated to that of a fundamental right.

The AG based his claims on the M.P. Sharma and Kharak Singh judgments, arguing that since a larger bench had found privacy was not a fundamental right, subsequent smaller benches upholding the right were not applicable. Sensing the need for reconciliation of the divergence of opinions on privacy, the Court referred this technical clarification on constitutionality of the right to a larger bench. The bench would determine whether the reasoning applied in M.P. Sharma and Kharak Singh were correct and still relevant in present day. The bench was set up not to not look into the constitutional validity of Aadhaar, but to consider a much larger question: whether right to privacy is a fundamental right and can be traced in the rights to life and personal liberty.

❖ FACTS OF THE CASE

In August 2017, an unanimous judgment by the Supreme Court of India in *Justice K.S. Puttaswamy (Retd) vs Union of India* is a resounding victory for privacy. The ruling is the outcome of a petition challenging the constitutional validity of the Indian biometric identity scheme Aadhaar.

The judgment's ringing endorsement of the right to privacy as a fundamental right mark a watershed moment in the constitutional history of India.

The one-page order signed by all nine judges declares:

"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."

The judgment, in which the judges state the reasons behind the one-page order, spans 547 pages and includes opinions from six judges, creating a legal framework for privacy protections in India. The opinions cover a wide range of issues in clarifying that privacy is a fundamental inalienable right, intrinsic to human dignity and liberty.

The decision is especially timely given the rapid roll-out of Aadhaar. In fact, the privacy ruling arose from a pending challenge to India's biometric identity scheme. Ambiguity on the nature and scope of privacy as a right in India allowed the government to collect and compile both demographic and

biometric data of residents. The original justification for introducing Aadhaar was to ensure government benefits reached the intended recipients. Following a rapid roll-out and expansion, it is the largest biometric database in the world, with over 1.25 billion Indians registered. The government's push for Aadhaar has led to its wide acceptance as proof of identity, and as an instrument for restructuring and facilitating government services.

❖ IDENTITY AND PRIVACY IN INDIA

Initiated as an identity authentication tool, the critical problem with Aadhaar is that it is being pushed as a unique identifier to access a range of services. The government continues to maintain that the scheme is voluntary, and yet it has galvanized enrollment by linking Aadhaar to over 50 schemes. Aadhaar has become the de-facto identity document accepted at private, banks, schools and hospitals. Since Aadhaar is linked to the delivery of essential services, authentication errors or deactivation has serious consequences including exclusion and denial of statutory rights. But more importantly, using a unique identifier across a range of schemes and services enables seamless combination and comparison of databases. By using Aadhaar, the government can match existing records such as driving license, ration card, financial history to the primary identifier to create detailed profiles. Aadhaar may not be the only mechanism, but essentially, it's a surveillance tool that the Indian government can use to surreptitiously identify and track citizens.

This is worrying, particularly in context of the ambiguity regarding privacy in India. The right to privacy for Indian citizens is not enshrined in the Constitution. Although, the Supreme Court has located the right to privacy as implicit in the concept of "ordered liberty" and held that it is necessary in order for citizens to effectively enjoy all other fundamental rights. There is also no comprehensive national framework that regulates the collection and use of personal information. In 2012, Justice K.S. Puttaswamy challenged Aadhaar in the Supreme Court of India on the grounds that it violates the right to privacy. The Court passed an interim order restricting compulsory linking of Aadhaar for benefits delivery, and referred the clarification on privacy as a right to a larger bench.

The delay in sorting out the nature and scope of privacy as right in India had allowed the government to continue linking Aadhaar to as many schemes as possible, perhaps with the intention of ensuring the scheme becomes too big to be rolled back. In 2016, the government enacted the 'Aadhaar Act' passing the legislation without any debate, discussion or even approval of both houses of Parliament. In April 2017, Aadhaar was made compulsory for filing income tax or PAN number application and the decision was challenged in Supreme Court. Defending the State, the Attorney-General of India

claimed that the arguments on so-called privacy and bodily intrusion is bogus, and citizens cannot have an absolute right over their body! The State's articulation is chilling, especially in light of the Human DNA Profiling Bill seeking the right to collect biological samples and DNA indices of citizens. Such anti-rights arguments are worth note because biometric tracking of citizens isn't just government policy - it is also becoming big business.

❖ AADHAR CARD PRIVACY PROBLEMS

Indian citizens have been required to submit their photograph, iris and fingerprint scans in order to access legal entitlements, benefits, compensation, scholarships, and even nutrition programs. Submitting biometric information is needed for the rehabilitation of manual scavengers, the training and aid of disabled people, and anti-retroviral therapy for HIV/AIDS patients. Soon police in the Alwar district of Rajasthan will be able to register criminals, and track missing persons through an app that integrates biometric information with the Crime and Criminal Tracking Network Systems (CCTNS).

These instances demonstrate how intrusive India's controversial national biometric identity scheme, better known as Aadhaar has grown. Aadhaar is a 12-digit unique identity number (UID) issued by the government after verifying a person's biometric and demographic information. As of April 2017, the Unique Identification Authority of India (UIDAI) has issued 1.14 billion UIDs covering nearly 87% of the population making Aadhaar, the largest biometric database in the world.

It is that enrollment reduces fraud in welfare schemes and brings greater social inclusion. Welfare schemes that provide access to basic services for marginalized and vulnerable groups are essential. However, unlike countries where similar schemes have been implemented, invasive biometric collection is being imposed as a condition for basic entitlements in India. The privacy and surveillance risks associated with the scheme have caused much dissension in India.

❖ TIMELINE OF EVENTS

HIV Positive people dropping out of treatment programmes because they fear Aadhaar data leaks (November 2017) There has been the spread of the linking of the patient identity cards of HIV positive patients, pushed for by the National Aids Control Organisation.
Large telco secretly opens bank accounts using Aadhaar-linked eKYC (December 2017)

In December 2017, it was revealed that the large telco Bharti Airtel made use of Aadhaar-linked eKYC (electronic Know Your Customer) to open bank accounts for their customers without their knowledge or consent.
Access to the details of 1 billion entries of the Aadhaar database available for only 500 rupees (January 2018) In January 2018, journalists found that, for 500 rupees (around $7USD), they were able to buy on WhatsApp access to a gateway that allowed them to access the personal details connected to any of the entries on the Aadhaar database - by entering any Aadhaar number, they could see details like the
A data leak on a utility company website made details of every Aadhaar holder available (March 2018) In March 2018, a security researcher discovered that the state-owned utility company Indane had access to the Aadhaar database via an API, but they did not secure this way of entry.
Widely-available software patch enables the creation of new people on the Aadhaar database (September 2018) In September 2018, a software patch was found by journalists to be widely available, that disabled or weakened the security features in the software used to enroll people on the Aadhaar database, potentially from anywhere in the world.

❖ SECURITY RISKS AND LIABILITY

A series of data leakages as above have raised concerns about which private entities are involved, and how they handle personal and sensitive data. In February, UIDAI registered a complaint against three companies for storing and using biometric data for multiple transactions. Aadhaar numbers of over 130 million people and bank account details of about 100 million people have been publicly displayed through government portals owing to poor security practices. A recent report from Centre for Internet and Society (CIS) showed that a simple tweaking of URL query parameters of the National Social Assistance Programme (NSAP) website could unmask and display private information of a fifth of India's population.

Such data leaks pose a huge risk as compromised biometrics can never be recovered. The Aadhaar Act establishes UIDAI as the primary custodian of identity information, but is silent on the liability in

case of data breaches. The Act is also unclear about notice and remedies for victims of identity theft and financial frauds and citizens whose data has been compromised. UIDAI has continued to fix breaches upon being notified, but maintains that storage in federated databases ensures that no agency can track or profile individuals.

After almost a decade of pushing a framework for mass collection of data, the Indian government has issued guidelines to secure identity and sensitive personal data in India. The guidelines could have come earlier, and given large data leaks in the past may also be redundant. Nevertheless, it is reassuring to see practices for keeping information safe and the idea of positive informed consent being reinforced for government departments. To be clear, the guidelines are meant for government departments and private companies using Aadhaar for authentication, profiling and building databases fall outside its scope. With political attitudes to corporations exploiting personal information changing the world over, the stakes for establishing a framework that limits private companies commercializing personal data and tracking Indian citizens are as high as they have ever been.

❖ MAIN ARGUMENTS AND PRIVACY QUESTION

The main privacy arguments of the petitioners were that this project forces the individual to part with biometric information (fingerprints and iris scan), and the authentication process is susceptible to misuse. Further, the information relating to different transactions across the life of the individual is connected to a central database which may enable the state to profile citizens, track movements, assess their habits and influence behavior. It was thus contended that the Aadhaar Act strikes at the fundamental right to privacy of the individual. The question before the court was whether the act is unconstitutional for this reason.

❖ THREE-PART TEST TO JUDGE THE REASONABLENESS OF THE INVASION TO PRIVACY

The landmark privacy judgment held that when a state action is challenged on the ground that it is violative of the right to privacy, then in order to determine the permissible limits of the invasion and the validity of the legislation, it has to be judged based on a three-part test comprising of the doctrine of proportionality. The court thus tested the project as such and found that it satisfied this test.

The test conducted by the court has been classified as such:

1. There must be a law, i.e., the action must be sanctioned by law.

2. The action must serve a legitimate state aim.

3. There must be proportionality, i.e., the extent of interference by such action should be proportionate to the need for such action. This part is then further sub-classified as under:

A. Legitimate goal stage: The measure restricting a right must have a legitimate goal.

B. Suitability or rationale connection stage: The measure must be a suitable means of furthering such goal.

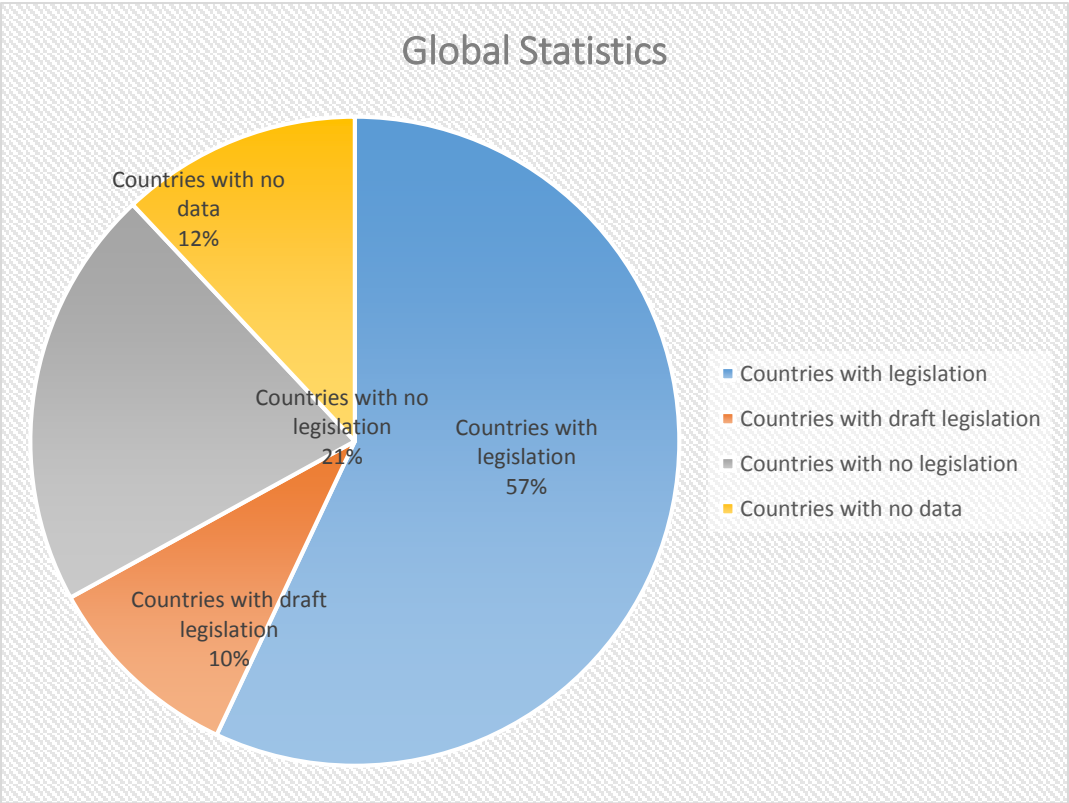
C. Necessity stage: There should be no other alternative which is less restrictive but equally effective.

D. Balancing stage: The action should not have a disproportionate impact on the holder of the right. This is also the stage which dominated the legal analyses by the court.

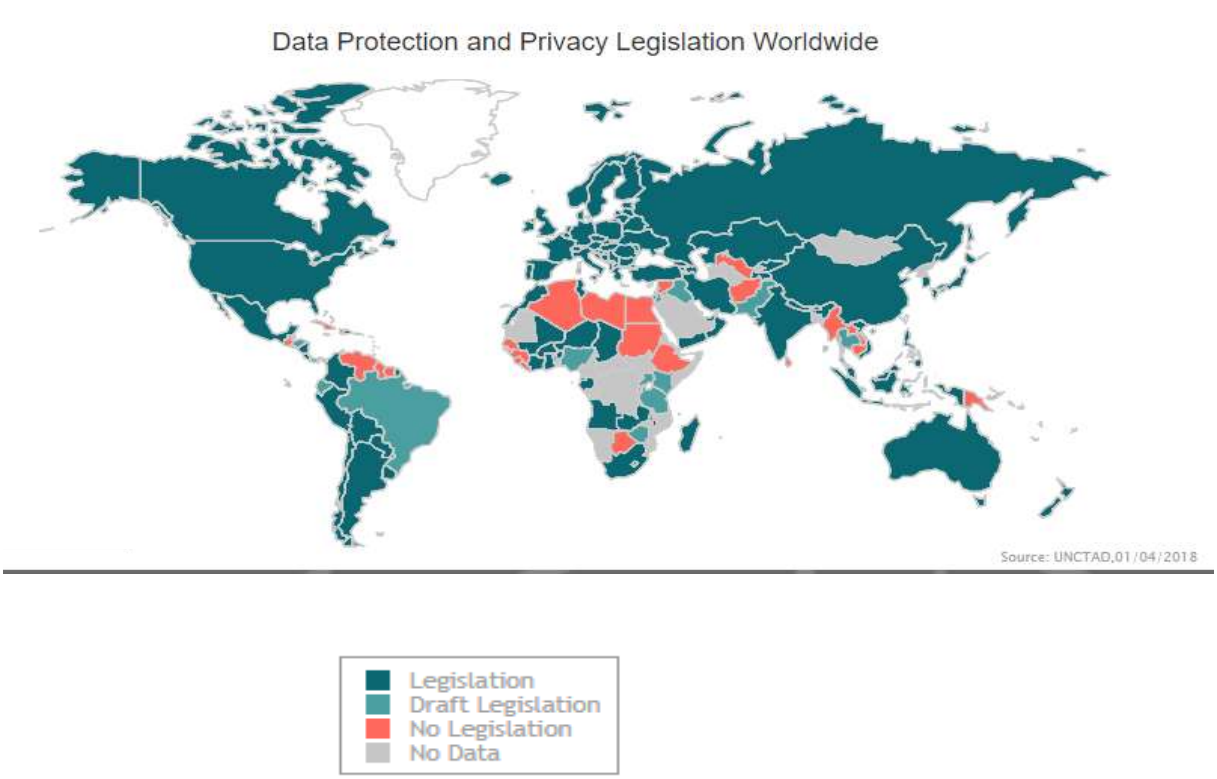
❖ LATEST DEVELOPMENTS

The Supreme Court of India on September 26, 2018, by a 4 to 1 majority, upheld the constitutional validity of the Aadhaar project, after some minor tweaks and suggestions. This 1148-page judgment was delivered after a 38-day hearing, the second longest hearing in the history of the court.

As given below the global statistics show that majority of the Countries already have legistlation for Data Protection but we are lacking behind in the same. This led to the development and Introduction of the **Personal Data Protection Bill, 2018** which is the most important implication of these landmark judgement. This judgement came along with their own set of effects on various businesses and organizations. The same has mentioned in detail.


Global Statistics
Countries with no data 12%
Countries with no legislation 21%
Countries with legislation 57%
Countries with draft legislation 10%
Countries with legislation
Countries with draft legislation
Countries with no legislation
Countries with no data

CHAPTER III: IMPLICATIONS OF THE JUDGEMENT



The most important implication of this judgement was the Introduction of the Data Protection Bill, 2018.

The transfer of personal data is currently governed by the SPD Rules (Sensitive Personal Data and Information, 2011) which has increasingly proved to be inadequate.

The proposed Data Protection Bill 2018 essentially makes individual consent central to data sharing. The report notes that the right to privacy is a fundamental right.

The Committee of Experts on a Data Protection Framework for India **(Chair: Justice B. N. Srikrishna)** submitted its report (the "**Report**") and draft Bill to the **Ministry of Electronics and Information Technology** on **July 27, 2018, the Personal Data Protection Bill, 2018** (the "**Bill**").

The Committee, chaired by Justice Srikrishna, was constituted by the Ministry of Electronics & Information Technology, Government of India to put together a draft of data protection law for India, to examine issues related to data protection, recommend methods to address them, and draft a data protection Bill. The Report elaborates on the Committee discussions and deliberations and throws light on the provisions of the Bill. The Bill may undergo further changes before it is adopted as law.

This is a keystone development in the evolution of data protection law in India. With India moving towards digitization, a robust and efficient data protection law was the need of the hour. The Bill has been drafted with an intention to fill in the vacuum that existed in the current data protection regime, and to enhance individual rights by providing individuals full control over their personal data, while ensuring a high level of data protection.

The Bill has been broadly based on the framework and principles of the General Data Protection Regulation (the "**GDPR**") recently notified in the European Union and on the foundation of the landmark judgement of the apex court: *Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors (W.P. (Civil) No. 494 of 2012),* wherein the Supreme Court of India upheld the right to privacy as a fundamental right under the Indian Constitution. The Bill shall come in supersession of Section 43A of the Information Technology, 2000 (the "**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "**IT Rules**") which was enacted under Section 43A of the IT Act.

Under Srikrishna Committee's draft, the 'right to be forgotten', is defined differently — right to restrict or prevent continuing disclosure of personal data. The process of justifying why the consumer does not want to continue giving consent is also long-winded.

❖ FEATURES AND OBSERVATIONS

- **Fiduciary relationship:** The Committee observed that the regulatory framework has to balance the interests of the individual with regard to his personal data and the interests of the entity such as a service provider who has access to this data. It noted that the relationship between the individual and the service provider must be viewed as a fiduciary relationship. Therefore, the service provider processing the data is under an obligation to deal fairly with the individual's personal data, and use it for the authorised purposes only.

- **Obligations of fiduciaries:** To prevent abuse of power by service providers, the law should establish their basic obligations, including:
    (i) the obligation to process data fairly and reasonably, and
    (ii) the obligation to give notice to the individual at the time of collecting data to various points in the interim.

- **Definition of personal data:** The Committee noted that it is important to define what constitutes personal information. It defined personal data to include data from which an individual may be identified or identifiable, either directly or indirectly.

- **Consent-based processing:** The Committee noted that consent must be treated as a pre-condition for processing personal data. Such consent should be informed or meaningful. Further, for certain vulnerable groups, such as children, and for sensitive personal data, a data protection law must sufficiently protect their interests, while considering their vulnerability, and exposure to risks online. Further, sensitive personal information should require explicit consent of the individual.

- **Non-consensual processing:** The Committee noted that it is not possible to obtain consent of the individual in all circumstances. Therefore, separate grounds are established for processing data without consent. The Committee identified four bases for non-consensual processing:
  (i) where processing is relevant for the state to discharge its welfare functions,
  (ii) to comply with the law or with court orders in India,
  (iii) when necessitated by the requirement to act promptly (to save a life, for instance), and
  (iv) in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer).

- **Participation rights:** The rights of the individual are based on the principles of autonomy, self-determination, transparency and accountability to give individuals control over their data categorised in three categories:
  (i) the right to access, confirmation and correction of data,
  (ii) the right to object to data processing, automated decision-making, direct marketing and the right to data portability, and
  (iii) the right to be forgotten.

- **Enforcement models:** The Committee also recommended setting up a regulator to enforce the regulatory framework. The Authority will have the power to inquire into any violations of the data protection regime, and can take action against any data fiduciary responsible for the same. The Authority may also categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to individuals. Such fiduciaries will be required to undertake additional obligations.

- **Amendments to Other Laws:** The Committee noted that various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data. These laws include:

  a) Information Technology Act, 2000, and the Census Act, 1948
  b) Aadhaar Act, 2016 to bolster its data protection framework.
  c) Right to Information Act, 2005

- **Rights of the individual:** The Bill sets out certain rights of the individual. These include:
  (i) right to obtain confirmation from the fiduciary on whether its personal data has been processed,
  (ii) right to seek correction of inaccurate, incomplete, or out-of-date personal data, and
  (iii) right to have personal data transferred to any other data fiduciary in certain circumstances.

- **Obligations of the data fiduciary:** The Bill sets out obligations of the entity who has access to the personal data (data fiduciary).

  These include:

  (i) implementation of policies with regard to processing of data,
  (ii) maintaining transparency with regard to its practices on processing data,
  (iii) implementing security safeguards (such, as encryption of data), and
  (iv) instituting grievance redressal mechanisms to address complaints of individuals.

- **Data Protection Authority:** The Bill provides for the establishment of a Data Protection Authority. The Authority is empowered to:

  (i) take steps to protect interests of individuals,
  (ii) prevent misuse of personal data, and
  (iii) ensure compliance with the Bill. It will consist of a chairperson and six members, with knowledge of at least 10 years in the field of data protection and information technology.

  Orders of the Authority can be appealed to an Appellate Tribunal established by the central government and appeals from the Tribunal will go to the Supreme Court.

- **Grounds for processing personal data:** The Bill allows processing of data by fiduciaries if consent is provided. However, in certain circumstances, processing of data may be permitted without consent of the individual. These grounds include: (ii) if necessary for any function of Parliament or state legislature, or if required by the state for providing benefits to the individual, (iii) if required under law or for the compliance of any court judgement, (iv) to respond to a medical emergency, threat to public health or breakdown of public order, or, (v) for reasonable purposes specified by the Authority, related to activities such as fraud detection, debt recovery, and whistle blowing.

- **Grounds for processing sensitive personal data:** Processing of sensitive personal data is allowed on certain grounds, including:
  (i) based on explicit consent of the individual,
  (ii) if necessary for any function of Parliament or state legislature, or, if required by the state for providing benefits to the individual, or
  (iii) if required under law or for the compliance of any court judgement.

- Sensitive personal data includes passwords, financial data, biometric data, genetic data, caste, religious or political beliefs, or any other category of data specified by the Authority. Additionally, fiduciaries are required to institute appropriate mechanisms for age verification and parental consent when processing sensitive personal data of children.

- **Transfer of data outside India:** Personal data (except sensitive personal data) may be transferred outside India under certain conditions. These include: (i) where the central government has prescribed that transfers to a particular country are permissible, or (ii) where the Authority approves the transfer in a situation of necessity.

- **Exemptions:** The Bill provides exemptions from compliance with its provisions, for certain reasons including:

  (i) state security,

  (ii) prevention, investigation, or prosecution of any offence, or

  (iii) personal, domestic, or journalistic purposes.

- **Offences and Penalties:** Under the Bill, the Authority may levy penalties for various offences by the fiduciary including
  (i) failure to perform its duties,
  (ii) data processing in violation of the Bill, and
  (iii) failure to comply with directions issued by the Authority. For example, under the Bill, the fiduciary is required to notify the Authority of any personal data breach which is likely to cause harm to the individual. Failure to promptly notify the Authority can attract a penalty of the higher of Rs 5 crore or 2% of the worldwide turnover of the fiduciary.

❖ **KEY OBSERVATIONS**

- **Wide Definition of Sensitive Personal Data**

The bill considers wide scope of sensitive personal data.

- **Data Localization**

Every data fiduciary is required to store one serving copy of the personal data on a server or data centre that is located within the territory of India. The data fiduciaries are likely to find this obligation onerous, as it will **increase operational costs** for most of them.

- **Scope of Applicability**

Under the Justice B. N. Sri Krishna Report, an exception has been made based on the principle of territoriality. The Report states that any entity located in India only processing personal data of foreign nationals not present in India may be exempted from the application of the Bill by the Central Government.

- **Definition of Critical Personal Data**

The Bill states that critical personal data shall be only processed in a server or data centre located in India. This effectively means that such data cannot be transferred to any country outside India. It may be a challenge for businesses to service Indian consumers solely through the data centres in India. Further, the Bill does not define the term critical personal data or give any guiding principles for its determination.

- **Excessive Liability**

The Bill imposes liability on the directors of a company or the officers in charge for the conduct of the business of the company at the time of commission of the offence.

Further, due to lack of clarity in the law, the directors and officers in-charge may be held liable to pay the same quantum of penalties as may be imposed on the company.

- **Repeal of Section 43A of IT Act and IT Rules**

The Bill comes in supersession of Section 43A of the Information Technology, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which was enacted under the same provision. There is lack of clarity on whether data fiduciaries need to have a separate privacy policy or whether the detailed notice requirements under the Bill would be sufficient compliance under the law.

- **Employment**

With the Bill coming into effect, it may pose a possible challenge for employers to continue retaining data of their former employees, obtained during the course of employment, post their separation from the employer.

- **Periodic Review of Stored Personal Data**

Under the Bill, the data fiduciaries are under an obligation to conduct periodic review of the personal data stored with them so that it is not retained beyond the period necessary for the purpose of processing.

- **Notice**

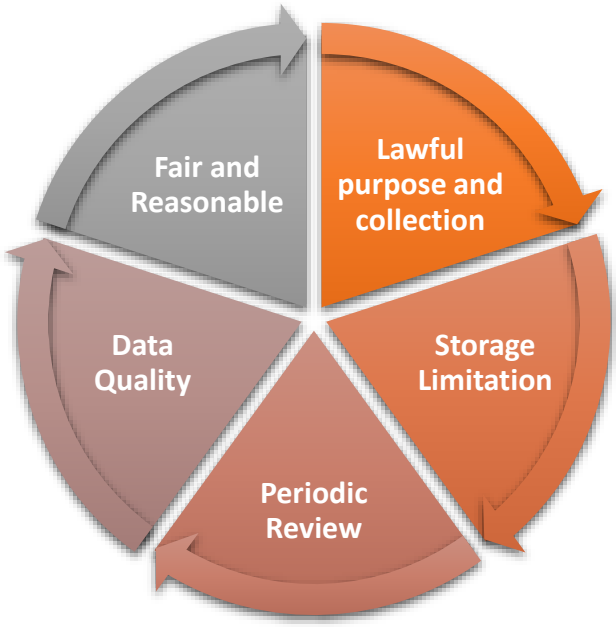
Under the Bill, the data fiduciary is under an obligation to provide the data principal with adequate notice before collection of personal data. The notice is required to be clear and concise, and if necessary and practicable, the notice shall be in multiple languages.

2.10 Data Protection Authority – Scope of authority

The Bill has vested the Authority with a wide range of administrative, discretionary, quasi-legislative and quasi-judicial powers. The exercise of powers vested in the Authority under the rules adopted under the Bill, should be in a manner to avoid any concentration of multiple conflicting powers and excessive delegation, thereby defeating the purpose of the Bill.

Further, the Report has suggested that the Bill shall not be applicable retrospectively i.e. it shall only be applicable to on-going or future processing activities and shall not apply to processing activities that have been completed before the law comes into effect.

❖ **DATA PROTECTION OBLIGATIONS**



CHAPER IV: EFFECTS ON BUSINESS: POSITIVE

❖ **Data localisation and transfer of personal data outside India – the boundaries**

The draft bill also proposes that data fiduciaries/companies save a local copy of all personal data that is stored outside the boundaries of India. Although this move could have some negative consequences, as discussed here, it would ensure effective enforcement of the law, reduce bottlenecks in dealing with foreign jurisdictions, and protect national security and interests. Further, in a move focused on protecting national interests and containing the risk of surveillance from foreign states on critical data, the draft bill prevents data fiduciaries from sending 'critical' personal data outside the territory of India. However, what constitutes personal data and 'critical' personal data is a decision that has been left up to the authority.

❖ **Tool to build trust**

The likely challenges for BFSI and FinTech companies in India to be privacy-ready are building and maintaining a culture of privacy and allocating budgets to increase technical and administrative procedures to ensure compliance. BFSI and FinTech companies will need to relook at their existing applications, policies, and external contracts to ensure the entire ecosystem understands, abides and is able to quickly adhere to any changes in the privacy law. But as it stands, an eeffective data privacy policy in place serves as a great tool to build trust and while compliance might add to operational costs in the beginning, it will be good for business in the long run.

❖ **Forensics**

An important aspect of forensics, i.e. electronic discovery and computer forensic procedures that have analysis of computer systems and data residing on these systems at their core, appear to be affected by the reading of the Bill. As most companies do not restrict their employees from storing personal data on office-provided laptops and other information assets, the Bill can apply to these being treated as stores of personal data and thereby requiring employees' consent for forensic processing and analysis of these systems. In a scenario where an employee or a set of employees are being investigated for non-compliance or fraud, the organisation would be forced to seek consent prior to any forensic analysis being performed, in addition to disclosing the reason for such analysis.

❖ **Demand of skilled privacy professionals**

The role of a data protection officer will gain great importance across the technology industry. We see a rapid increase in demand of skilled privacy professionals and specialists that are equipped to handle compliance requirements coming from various privacy regulations around the world.

❖ **Data Portability**

Every person shall, as and when required, receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to data portability to another data controller without any hindrance.

❖ **Special provisions for Sensitive personal data**

Sensitive personal data shall not be processed unless express, affirmative and explicit written consent of the person subject to data collection has been obtained through letter or fax or email from the said person.

No sensitive personal data shall be processed for any purpose apart from for the specific purpose for which it was collected and/or implementation of welfare schemes and social protection laws.

If sensitive personal data has been collected by various government agencies, institutions, authorities or private companies, partnerships or any other body corporate. for a specific purpose or as a part of a statutory or legal requirement and any form of collaborating, converging or monitoring between or individually by entities shall be expressly barred if it amounts to or reasonably lead to —

a) individual profiling except for circumstances of reasonable restriction; or
b) mass profiling or profiling of certain group or class of persons without any lawful reason or adequate basis; or
c) unlawful access by third parties.

It shall be the duty of the data controller or processor, as the case may be, to ensure that the sensitive personal data is collected, stored or processed, in accordance with this Act with reasonable advanced security measures and safeguards to ensure the safety of such data.

❖ **Notification of breach**

It shall be the duty of the data controller and data processor, as the case may be, in case of any breach, unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental), or other reasonably foreseeable risks of personal data, to notify to the person who is the subject of such personal data as well as the Authority and take adequate steps to mitigate any harm or damage of the data security breach within seven days.

❖ **Protecting and Improving the Business Scenario:**

Once the Business Houses and Corporates becomes compliance friendly with the data protection bill which is an outcome of Right to Privacy the customers would start getting more reliant on the business practices and thereby they would feel protected and this in turn would help in improving the business scenario.

❖ **Reducing Crime, Corruption and violence:**

The legal regulation would bring about a dramatic reduction in crime, corruption and violence at all levels of business and thereby bringing in better transparency and governance.

The best available evidence suggests that prohibition and aggressive law enforcement measures are actively counterproductive, unintentionally generating increases in violence and crime.

❖ **Improving Security and Development:**

Right to Privacy would bring about the greater security and development for the business and corporates as the data protection would play a vital part in this motive.

❖ **Protecting the Human Rights and thereby Business would earn goodwill in the market:**

The company which follows the law in latter and spirit and adhere to the compliances always enjoy the goodwill and better standing in the market.

❖ **Encouraging safe work practices:**

Safe working practices are encouraged in all aspects of businesses, from health and safety through to employee wellbeing. This same concept should apply for your data, and by enforcing security when it comes to handling data, sensitive or other, you have employees who are more informed about managing and storing that information most appropriately. Data is the backbone that makes up many customer-focused businesses, and should never be a second thought.

❖ **Following the legal guidelines:**

No matter what kind of data you're storing on-site or through your company's servers, whether it's your payroll, information and other data from your customers or other materials that can affect the day-to-day work of your employees, keeping your data safe should be a number one priority for any company. With the proposed Data Protection Bill soon proposed to be effected keeping your data protected will be more than just a moral judgement – it will be a legal requirement.

❖ **Business Data Privacy Doesn't Just Protect Customers:**

Businesses often treat security as a series of special measures to protect certain information, but it's usually easier to be secure across the board than to only protect data in certain narrow circumstances. Data security isn't just a matter of installing tools and issuing a few memos — it requires you to review and categorize all your data, write tough policies, and train and retrain your workers until security best practices are part of everything they do.

Implementing strong, organization-wide privacy policies and practices will help protect intellectual property and trade secrets, along with customer relationships. If you confine your efforts to a small subset of highly valuable information, or pick user-unfriendly tools like secure client portals, you'll be much more likely to fall victim to low adoption rates, poor follow-through or plain old human error.

❖ **Protect your brand:**

When preparing for the worst, businesses should develop a communications strategy that works in conjunction with its IT-response plan. Otherwise, you risk a disjointed, inconsistent and delayed response to issues or crises. It is also imperative to align how your organization will communicate with stakeholders. This will reduce the need for real-time decision-making in an actual crisis, as well as help limit inappropriate responses. Finally, practice makes perfect. Running a cybersecurity crisis simulation will help you identify flaws and gaps in your process, and better prepare your teams for such a pressure-cooker situation when it hits.

❖ **Privacy matters to the growth of your business:**

Safeguarding customer privacy is more than a protective measure; it is also a strategic opportunity for brand growth and a potential business opportunity for startups and entrepreneurs, as well as large companies.

CHAPER V: EFFECTS ON BUSINESS: NEGATIVE

❖ **Cost of Compliance:**

A compliance cost is expenditure of time or money in conforming with government requirements such as legislation or regulation. For example, Data Protection Bill is the outcome of Right to Privacy. Once it becomes a law the business entities and the companies will have to adhere to its requirements. This may necessitate them having to employ someone skilled in this field, which would be regarded a compliance cost.

Compliance costs normally include all costs associated with obeying the law, including planning and administration, in addition to the direct time and money spent filing paperwork.

❖ **Effect on Start-ups:**

With ease of doing business being still relatively difficult for start-ups; creation of an additional regulator in the form of a Data Protection Authority will make things much more difficult for Indian tech start-ups, said industry body, Internet and Mobile Association of India (IAMAI) after a consultation session with its members on the impact of the draft Personal Data Protection Bill, 2018.

The bill submitted to the government by a high-level expert group headed by former Supreme Court judge B.N. Srikrishna on 27 July proposes setting up of a Data Protection Authority of India (DPA), an independent regulatory body responsible for the enforcement and effective implementation of the law, consisting of a chairperson and six whole-time members. In case of any appeal against an order of the DPA, an appellate tribunal should be established or an existing appellate tribunal should be granted powers to hear and dispose of any appeal, said the expert panel in its report submitted along with the draft bill.

❖ **Use of data analytics by companies to detect and prevent fraud:**

Another aspect is the use of data analytics by companies to detect and prevent fraud. For example, details provided by vendors may be analysed against details of employees to identify if there may be an underlying conflict of interest. The Bill suggests a need to seek consent from both parties as there is some guidance on data belonging to other categories that could be termed as personal information. In such a case, organisations may find it challenging to undertake proactive fraud risk management efforts, thereby running a risk of violating clauses under Companies Act 2013 (wherever applicable) that refer to fraud risk management.

While the Bill in its current form is a step in the right direction, some aspects may need to be considered for amendment prior to presenting it for enactment.

❖ **Ambiguity in Data Protection Bill could lead to complications:**

It is unclear to what extent consent would be necessary and what items it may cover. Would consent be required for accessing items such as payslips, which are originated by the organization yet can be categorized as sensitive personal information? How about copies of bank statements that an employee may have saved in office laptop without informing the company? Would they also come under scrutiny? It is likely that in anticipation of finding personal information, companies may be forced to work with the assumption that such information may be present on the systems used by the target employee and, as a cautionary measure, seek consent. Considering that in most forensic investigations, evidence is discovered through digital forensic procedures, the fraud management efforts of a company could get severely impacted if the target of the investigations declines consent. Worse, such a target may continue to engage in malpractice, taking advantage of the consent clause in the Bill.

❖ **Effect on Forensics:**

An important aspect of forensics, i.e. electronic discovery and computer forensic procedures that have analysis of computer systems and data residing on these systems at their core, appear to be affected by the reading of the Bill. As most companies do not restrict their employees from storing personal data on office-provided laptops and other information assets, the Bill can apply to these being treated as stores of personal data and thereby requiring employees' consent for forensic processing and analysis of these systems. In a scenario where an employee or a set of employees are being investigated for non-compliance or fraud, the organization would be forced to seek consent prior to any forensic analysis being performed, in addition to disclosing the reason for such analysis.

❖ **Business Houses could find it more stringent to follow:**

One of the things that good businesses prize is predictability. Every startup is a gamble, and adding profound regulatory uncertainty to the mix is not liable to convince a VC to cut you a cheque. The current data protection regime is so far behind the curve when it comes to the way data is actually collected and used now that it leaves far too many legal and ethical questions unanswered.

This law should mark a turnaround point for businesses – they need to start taking privacy seriously

and it gives them a template for how to do that. There will now be a clear imperative, in the form of penalties and potential enforcement action, to ensure that engineers and product managers think about privacy at all stages of product design and implementation. Some of the principles such as consent and purpose limitation already existed, but setting up a DPA means that they are now actionable. Having a DPA also means that jurisprudence on what terms such as "fair and reasonable" mean and what the scope of "personal data" is, will hopefully evolve. While all of this will mean increases in compliance costs in the short term, the long term benefits should certainly justify this.

- **Technical and Process Change:**

A slew of new rights, including the right to be forgotten, right to correction, and the right to data portability, need to be implemented by online platforms. This could mean significant technical and process changes.

- **Additional Cost of Employment:**

Companies need to appoint data protection officers whose job it will be to ensure compliance with the law and act as an interface with the DPA.

- **Regulatory Body:**

Data Protection Authority (DPA): There's a new regulator on the block and it's going to be a powerful one, with the ability to impose significant fines and extraterritorial authority.

- **New standards to be followed:**

All data processing needs to be carried out in a "fair and reasonable manner" and "privacy by design" needs to be incorporated into all platforms and products.

- **Purpose limitation**:

Personal data can be processed only for purposes that are clear, specific and lawful. Data processing must only take place for the purpose specified or for an incidental purpose that can be reasonably expected.

- **Fear of Curbing Innovation:**

The bill which has been put up for public comments and needs parliamentary approval to become an Act, also proposes localization of personal data. The members of the association who are mid-sized start-ups with ambitions to expand in the overseas market feared that their plans may be scuttled by the provisions of data localization.

"Other countries where they are expanding may retaliate by demanding reciprocal data localization. Data localization also forces Indian start-ups to look for more expensive and inefficient local solutions," IAMAI said.

- **Time Constraints:**

Those activities which were getting completed by a thumb impression Aadhar linked KYC may now be again revised to the physical paper based KYC Verification and which in turn could lead to time constraints.

- **No Uniformity:**

As it is said that the customer will have a choice whether to make a Aadhar linked KYC or not. If some customer opts for it and the other does not then it would lead to a mess for the companies and they would not be able to adopt uniformity in their process.

- **Impact on Communication services:**

Existing privacy laws under the Information Technology Act and the IT Reasonable Security Practices Rules do not apply to all the SMSes, contact lists, and other data in the possession of communication services like WhatsApp. They only cover 'sensitive personal data', a limited category of data like biometric data, financial data, sexual orientation, and so on.

In the absence of an alternative remedy, the WhatsApp Facebook case before the SC will determine if communication services like WhatsApp are a 'private company performing a public function'. This verdict will impact all similar services like Hike, Telegram, Skype and so on, and any directions passed will be applicable to them as well. This gives hope for immediate relief from any violative privacy practices, without having to wait for the data protection law to be framed.

- **Impact on *Job Portals:***

Recent reports allege that **Monster.com sold user data to third parties**. An enquiry has been ordered into this by a court, stating that such information cannot be shared without 'informed consent'. Though people expect data on such portals to be shared only with prospective employers, there is nothing to prevent the sharing with anyone.

The data in the possession of such job portals, such as professional qualifications and experience, are not protected under the IT Rules, leaving it to be decided by the Terms and Conditions of the website. Section 72A of the IT Act is unlikely to provide protection against such practices if the T&Cs of the company permit it, as is often the case. A data protection law, again, can force a change in such practices.

- **Impact on *Matrimonial websites:***

Matrimonial websites can lead to a host of privacy violations, including sale of data, identity theft using that data, and so on. There was a report was of matrimonial websites specialising in divorcees, acquiring **information illegally of new divorcees from matrimonial courts.**

Such illegal acquisition of data and leakage of data can be addressed by a data protection law, since no data can be taken without the person's consent. At this point, it isn't clear what the provisions of the data protection act will be. Hong Kong's privacy laws, for example, have strict laws against direct marketing, with penalties of HK$500,000. Such provisions can prevent such violations.

- **Impact on *Insurance sector:***

The insurance sector is highly regulated. Persons employed in this field are required to disclose a huge amount of data, which is essential to maintain the trust and integrity needed in this highly sensitive field. However, provisions for **protecting against privacy violations are missing**.

A data protection law can remedy such lacunae in insurance laws. In addition, the fundamental right to privacy may be enforceable directly against certain insurance companies such as LIC, which is established by statute, making it a statutory corporation, and thus a state authority.

❖ **Impact on *Banking sector:***

The situation in the banking sector is similar to the insurance sector. Some banks like the State Bank of India are, like LIC, also established by statute. Some banking laws, however, provide people with the option of approaching either the banking ombudsman or the RBI for privacy violations.

For example, under the Credit Information Companies Regulations, 2006, an individual has the right to approach the RBI for a privacy violation by a Credit information company. Case law has also established that banks have a duty of secrecy towards their customers established under contract. In addition, the IT Act will also apply for disclosure of financial data.

If all such remedies are inadequate, then the data protection law, and finally the direct enforcement of the fundamental right to privacy can be turned to.

❖ **Impact on *M-wallets:***

In the case of privacy violations by m-wallets, there are certain remedies — the IT Act for disclosure of sensitive data including financial data, and for disclosures in breach of contract, the RBI allows recourse to the banking ombudsman for redressal of grievances under the Circular on **Pre-paid Payment Instruments**, and the Draft Meity Rules for PPIs require a Grievance Officer to resolve customer grievances. When these remedies are inadequate, the data protection law can be turned to.

❖ **Take it or leave it approach may no longer work:**

While the data protection act, when enacted, will finally define the extent of protection available, private entities can be expected to no longer be able to take the take-it-or-leave-it approach to their services. The Supreme Court in its right to privacy verdict, in particular, Justice SK Kaul's verdict, has laid huge emphasis on the importance of informational privacy in the digital change.

Soon, a change should be seen in the privacy practices of private companies, with privacy practices tailored to the expected law and the fundamental right to privacy

CHAPTER VI: KEY QUESTIONS ANSWERED BY THE JUGEMENT

Q.1 Whether the Aadhaar Act could be passed as 'Money Bill' within the meaning of Article 110 of the Constitution? (Question on validity of Adhar Act)

Ans. We, thus, hold that the Aadhaar Act is validly passed as a 'Money Bill'

Q.2 Whether Section 139AA of the Income Tax Act, 1961 is violative of right to privacy and is, therefore, unconstitutional? (Question on validity of PAN)

Ans. Even after judging the matter in the context of permissible limits for invasion of privacy, namely: (i) the existence of a law; (ii) a 'legitimate State interest'; and (iii) such law should pass the 'test of proportionality', we come to the conclusion that all these tests are satisfied.

The dissenting judgment, Justice Chandrachud said that the seeding of Aadhaar in PAN cards depends on the constitutional validity of the Aadhaar legislation itself and does not stand independently as the Act is unconstituional as a Money Bill.

Q.3 Whether Rule 9 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and the notifications issued thereunder which mandates linking of Aadhaar with bank accounts is unconstitutional? (Question on linking Aadhaar to bank accounts)

Ans. We hold that the provision in the present form does not meet the test of proportionality and, therefore, violates the right to privacy of a person which extends to banking details.

Q.4 Whether Circular dated March 23, 2017 issued by the Department of Telecommunications mandating linking of mobile number with Aadhaar is illegal and unconstitutional? (Question on making Aadhaar mandatory for SIM card registration)

Ans. Circular dated March 23, 2017 mandating linking of mobile number with Aadhaar is held to be illegal and unconstitutional as it is not backed by any law and is hereby quashed.

CHAPTER VII:

CONCLUSION

With the recognition of privacy as a basic and fundamental right of an individual, India definitely cannot lag behind. The judgment of the Supreme Court is correct and true and with the growing information technology, privacy needs to be fundamental right. However, it is also true that stringent laws need introduction after this.

Also, Aadhaar is now mandatory for a large proportion of India's population. That means, for anyone who is claiming their welfare entitlements, and for anyone who is eligible to pay income tax, they must surrender their biometrics to a scheme that is, at the moment, lightly regulated by law.

To put this into a larger context, the Supreme Court majority seems to imagine that Aadhaar is a sophisticated version of the US Social Security Number or the UK's National Insurance Number, where it is appropriate to be made mandatory for an individual's financial interactions with the state (e.g. tax, welfare) but not other things. But first, even if this was true, Aadhaar should have more safeguards on it akin to safeguards elsewhere in the world. And second, Aadhaar isn't a single numbering system alone, it is a giant centralised biometric database. Questions of constitutionality, proportionality, and necessity need to consider these realities in great detail, including interrogating claims of technical efficiency and technological capabilities.

The Aadhaar project has survived, but the right to privacy and choice of the beneficiaries has suffered. The facts were not to the liking of the majority and they failed the proportionality test determined by the majority judgment. Paradoxically though, the dissent gives a choice to both the government and the legislature. The government may either feel vindicated and be content by fixing the glitches that the majority judgment pointed out, or it may rise to the occasion and look at the issue afresh from the dissent’s perspective. The legislature also has a choice to either come up with a data privacy law based on the lower standards of privacy protection set up by the majority or to follow the dissent and use it as the foundation of the upcoming data privacy law.

The lead judgment calls for the government to create a data protection regime to protect the privacy of the individual. It recommends a robust regime which balances individual interests and legitimate concerns of the state. Justice Chandrachud notes, "Formulation of a regime for data protection is a complex exercise that needs to be undertaken by the state after a careful balancing of requirements of privacy coupled with other values which the protection of data subserves together with the legitimate concerns of the state." For example, the court observes, "government could mine data to ensure resources reached intended beneficiaries." However, the bench restrains itself from providing guidance on the issues, confining its opinion to the clarification of the constitutionality of the right to privacy.

The judgment will also have ramifications for a number of contemporary issues pending before the supreme court. In particular, two proceedings—on Aadhaar and on WhatsApp-Facebook data sharing—will be test grounds for the application and contours of the right to privacy in India. For now, what is certain is that the right to privacy has been unequivocally articulated by the highest Court. There is much reason to celebrate this long-due victory for privacy rights in India. But it is only the first step, as the real test of the strength of the right will in how it is understood and applied in subsequent challenges.

❖ BIBLIOGRAPHY

Legal References:

(a) Right to Privacy – Judgement

i) Writ Petition (Civil) No 494 Of 2012, Justice K S Puttaswamy (Retd.), And Anr. Petitioners Versus Union Of India And Ors Respondent
https://www.sci.gov.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

ii) Writ Petition (Civil) No. 494 Of 2012, Justice K.S. Puttaswamy (Retd.) And Another Petitioner(S) Versus Union Of India And Others Respondent(S)
https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

(b) Data Protection Bill

http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

(c) General Data Protection Regulations

https://gdpr-info.eu/

Websites:

https://www.pwc.in/consulting/cyber-security/blogs/decoding-the-personal-data-protection-bill-2018-for-individuals-and-businesses.html

https://www.deccanherald.com/business/economy-business/personal-data-protection-bill-697953.html

https://economictimes.indiatimes.com/tech/internet/proposed-data-protection-bill-2018-ambiguous-says-pwc-assocham-finding/articleshow/65529136.cms

https://inc42.com/features/the-personal-data-protection-bill-2018-does-everything-but-protect-personal-data/

https://factordaily.com/what-works-and-hurts-business-india-new-data-protection-bill/

https://www.pwc.in/consulting/cyber-security/blogs/decoding-the-personal-data-protection-bill-2018-for-individuals-and-businesses.html

https://www.deccanherald.com/business/economy-business/personal-data-protection-bill-697953.html

https://inc42.com/features/the-personal-data-protection-bill-2018-does-everything-but-protect-personal-data/

https://factordaily.com/what-works-and-hurts-business-india-new-data-protection-bill/

Newspaper Articles (Weblink):

https://www.livemint.com/Companies/LVim5cnEHcCFTPBSBvJd6M/Startups-likely-to-be-hit-by-Data-Protection-Bill-IAMAI.html

https://www.financialexpress.com/opinion/data-protection-bill-whom-does-it-really-protect/1281828/

https://www.livemint.com/Companies/LVim5cnEHcCFTPBSBvJd6M/Startups-likely-to-be-hit-by-Data-Protection-Bill-IAMAI.html

https://www.financialexpress.com/opinion/data-protection-bill-whom-does-it-really-protect/1281828/

https://economictimes.indiatimes.com/tech/internet/proposed-data-protection-bill-2018-ambiguous-says-pwc-assocham-finding/articleshow/65529136.cms