**INTRODUCTION**

Right to privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties. Privacy underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the Modern age. Almost all countries in the world recognizes, right of privacy in their constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. However, in many of the countries where privacy is not explicitly recognized in the constitution, such as the United States (U.S.), Ireland and India, the Court have found that right in other provisions.

**RIGHT TO PRIVACY UNDER HUMAN RIGHTS DISCOURSE**

In many Countries, International agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights were adopted into law. It was in during 1970s, countries of the world began adopting broad laws intended to protect individual privacy. Throughout the world, there is a general movement towards adopting comprehensive privacy laws that set a framework for protection.

Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of privacy in early Hebrew culture, classical Greece and ancient China. These protections mostly focused on the right to solitude. Definitions of privacy vary widely according to context and environment. In the recent past, with the increasing sophistication of information technology with its capacity to collect, analyze and disseminate information on individuals introduced a sense of urgency to the demand for privacy legislation. Again, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers dramatically increased the level of information generated by each individual. Computers linked together by high-speed networks with advanced processing systems can create comprehensive dossiers on any person without the need for a single central computer system.

New technologies developed by the defense industry are spreading into law enforcement, civilian agencies, and private companies1. In view of the recent technological innovations and fast progress of information transfer, sharing, concern over privacy violations are now greater than at any time in recent history. Under these circumstances, the people throughout the world express fears about encroachment on privacy, prompting an unprecedented number of nations to pass laws specifically protecting the privacy of their citizens. Human rights groups are concerned that much of this technology is being exported to developing countries that lack adequate protections2

In broad sense, all human rights are aspects of the right to privacy3. Privacy can be defined as a fundamental though not an absolute human right. In this connection, it is to be noted that the developments of communication technologies have been among the

1. Simon Davies, Re-engineering the Right to Privacy: How Privacy has been Transformed from a Right to a Commodity, in Technology and Privacy The New Landscape 143
2. David Banisar and Simon Davis, Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, And Surveillance Laws And Developments, https://poseidon01.ssrn.com/ delivery.php?I Retrieved on 31-7-2017
3. Fernando Volio, Legal Personality, Privacy and the Family, The International Bill of Rights, Henkin ed. 1981.

law[[1]](#footnote-1).” There is also a right of privacy guaranteed by Indian laws. Unlawful attacks on the honour and reputation of a person can invite an action in tort and/or criminal law[[2]](#footnote-2). The Public Financial Institutions Act of 1993 codifies India's tradition of maintaining confidentiality in bank transactions. However, National Policy on Information Security, Privacy and Data Protection Act for handling of computerized data has examined the U.K. Data Protection Act as a model and recommended a number of cyber-laws including ones on privacy and encryption. Based on this and also by examining the suitability to Indian context, the Indian Information Technology Act, 2000 was enacted. Wiretapping is regulated under the Indian Telegraph Act of 1885. An order for a tap can be issued only by the Union Home Secretary or his counterparts in the States. A copy of the order must be sent to a review committee and directed to be set up by the High Court. Tapped phone calls are not accepted as primary evidence in Indian Courts.

With the expansion of scientific advancement and invention, if new electronic gadgets, using biometric technology to identify and monitor people raises human rights concerns. The implications of usage of biometrics are often associated with intrusions into privacy. In biometric system, the personal and permanent nature of the physiological features analyzed raising an inherent tension with privacy interests. In circumstances where biometrics are applied in a surveillance context, concerns of Human-beings for privacy naturally increase.

The term and technology Biometrics refers to a process of recording, measuring, and analyzing a range of human physiological features. The scope of features to which biometrics may be directed is “all encompassing, and includes appearance, behaviour, and cognitive state[[3]](#footnote-3)”. In species, certain physiological features are permanent, unique, and universal. They are known as “biometric characteristics.” Those characteristics are typically measured by a sensor array and stored on a database as a “template” and a template enables to identify a person, or to verify a person's identity, at a subsequent time. In an identity verification application, a person enrolls in the system, and his identifying data are measured and recorded in a database or on a document. To confirm the person’s identity later, his identifying data are measured again and compared with the original. This is known as one-to-one matching. Biometric identification usually applies to a situation where an organization needs to identify a person. The organization captures a biometric from that individual and then searches a biometric repository in an attempt to correctly identify the person.

In India, in the recent times, biometric identification project has been launched and biometrics has been trending the popularity charts for quite a while, and analytics brings an insider peek at this newly gravitating technology — that implies metrics related to human characteristics. The various technologies for identification, now one come across fingerprint scanning, face recognition, voice recognition, iris scan and more not just recently but way back in 1950s or 60s in popular scientific movies like Star Trek. While these caught our imaginations for quite long, it is remarkable as to how these technologies have transcended from showbiz into the world of reality.

In India, Aadhaar is a 12-digit unique identity number issued to all Indian residents based on their biometric and demographic data. Aadhaar card is essentially an identification document issued by the UIDAI after it records and verifies every resident Indian citizen’s details including biometric and demographic data. Aadhaar is not meant to replace existing identification documents like PAN, passport, driving license etc. However, it can be used as a single identification document. Banks, financial institutions and telecom companies can also use it as a Know-Your-Customer (KYC) verification mode and maintain profiles. The data is collected by the Unique Identification Authority of India (UIDAI), a statutory authority established in January 2009 by the government of India, under the jurisdiction of the Ministry of Electronics and Information Technology, following the provisions of the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016.

The Aadhaar program is one of the technology success stories of India, and is an initiative unparalleled in scope anywhere else in the world. India is leading the way in the implementation of a national identification program linked to biometric data Aadhaar is the world's largest biometric ID system, with over 1.20 billion enrolled members as on 31-12-2017 representing over 99% of Indians. The card is meant to streamline bureaucratic processes, for better governance, delivering a range of services to the citizens as well as distribution of benefits and subsidies. According to Paul Romer, the chief economist at the World Bank, Aadhar is bloomberg that a worldwide standardised system on the lines of Aadhaar will benefit everyone on the planet. “The system in India is the most sophisticated I have seen. It’s the basis for all kinds of connections that involve things like financial transactions.

**CREATION OF UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UDIDAI):**

Prior to its establishment as a statutory authority, Unique Identification Authority of India (UIDAI) was functioning as an attached office of the then Planning Commission[[4]](#footnote-4) vide its Gazette Notification No.-A-43011/02/2009-Admn.I) dated 28th January, 2009. Later, on 12 September 2015, the Government revised the Allocation of Business Rules to attach the UIDAI to the Department of Electronics & Information Technology of the then Ministry of Communications and Information Technology.

The statement of objects and reasons for enactment of the Act reads thus: An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto. This Act consists of 59 Sections spared into eight chapters.

Unique Identification Authority of India (UIDAI) was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India to:

1. Robust enough to eliminate duplicate and fake identities, and
2. Can be verified and authenticated in an easy, cost-effective way.

The first UID number was issued on 29 September 2010 to a resident of Nandurbar, Maharashtra. By the end of January, 2017, over 99% of Indians aged 18 and above now have Aadhaar cards as more than 1,110 million residents have enrolled themselves for the unique identification number. This is further accelerated after demonetization, Aadhaar generation and its use for financial transactions saw a substantial jump due to the demonetization effect also and the Government is encouraging the use of AadhaarPay, a merchant version of Aadhaar-enabled payment system.

The Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016 is a money bill of the Parliament of India. It aims to provide legal backing to the Aadhaar unique identification number project. It was passed on 11 March 2016 by the Lok Sabha. Certain provisions of the Act came into force from 12th July 2016 to 12th September 2016. Most of the provisions of the Bill have been borrowed from the previous National Identification Authority of India Bill, 2010. The major difference is that the three-member committee called the Identity Review Committee of the previous bill was removed in the new bill. Section 8 of Aadhaar Act is significantly different from that of NIAI bill, 2010. While the NIAI bill allowed the authentication limited to the biometric match only with Yes/No option, the Aadhaar Act allows the requesting agency/person to ask for other information too, pertaining to the person’s identity. **AADHAAR ACT, 2016:**

Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also required to ensure the security of identity information and authentication records of individuals.

Chapter – I under sections 1 and 2 deals with the nomenclature and definitions of the Act. Chapter – II deals with enrolment of Aadhar number procedure, the properties of Aadhaar number, providing Special measures for issuance of Aadhaar number to certain category of persons and Update of certain information. Chapter – III provides for authentication. According to Section 7 of the Act, the Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment. Thus, this provision deals with Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc. Section 8 deals with the authentication of Aadhaar number. According to this section, the Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations. The Clause 8 (4) states that UIDAI may share identity information, but it cannot share the biometric information. The Section 9 states that Aadhaar is not a proof of citizenship or domicile. Section 10 provides for Central Identities Data Repository. The UIDAI Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

Chapter – IV of the Act deals with the constitution of Unique Identification Authority of India. Unique Identification Authority of India (“Authority/UIDAI”) has its Headquarters in New Delhi and eight Regional Offices (ROs) across the country. UIDAI has two Data Centres, one at Hebbal (Bengaluru), Karnataka and another at Manesar (Gurugram), Haryana. In accordance with section 11 of the Act, the Central Government shall, by notification, establish an Authority to be known as the Unique Identification Authority of India to be responsible for the processes of enrolment and authentication and perform such other functions assigned to it under this Act. Section 12 provides for Composition of Authority. The Authority shall consist of a Chairperson, appointed on part-time or full- time basis, two part-time Members, and the Chief Executive Officer who shall be Member-Secretary of the Authority, to be appointed by the Central Government. So far as the Qualifications for appointment of Chairperson and Members of Authority are concerned, the Chairperson and Members of the Authority shall be persons of ability and integrity having experience and knowledge of at least ten years in matters relating to technology, governance, law, development, economics, finance, management, public affairs or administration. Term of office and other conditions of service of Chairperson and Members and the Chairperson and the Members appointed under this Act shall hold office for a term of three years from the date on which they assume office and shall be eligible for re-appointment. (Section 14) Section 15 provides procedure for Removal of Chairperson and Members and Section 6 with restrictions on Chairperson or Members on employment after cessation of office.

The functions of the Chairperson are concerned, Section 17 stipulates that the Chairperson shall preside over the meetings of the Authority, and without prejudice to any provision of this Act, exercise and discharge such other powers and functions of the Authority as may be prescribed. The Chief Executive Officer who shall be full time officer has been entrusted with day to day administration of the authority which include (a) the day-to-day administration of the Authority; (b) implementing the work programmes and decisions adopted by the Authority; (c) drawing up of proposal for the Authority’s decisions and work programmes; (d) the preparation of the statement of revenue and expenditure and the execution of the budget of the Authority; and (e) performing such other functions, or exercising such other powers, as may be specified by regulations. Section 19 makes it mandatory that the Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings, including quorum at such meetings, as may be specified by regulations.

**UIDAI – POWERS AND FUNCTIONS UNDER AADHAAR ACT, 2016:**

Detailed powers and functions of the Authority are enumerated in Section 23 of the Act. Section 23 (1) The Authority shall develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and perform authentication thereof under this Act (2) Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—

1. Specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;
2. Collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;
3. Appointing of one or more entities to operate the Central Identities Data

Repository;

1. Generating and assigning Aadhaar numbers to individuals;
2. Performing authentication of Aadhaar numbers;
3. Maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;
4. Omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations;
5. specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;
6. Specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;
7. Establishing, operating and maintaining of the Central Identities Data Repository;
8. Sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;
9. Calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;
10. Specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;
11. Specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder;
12. Levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;
13. Appointing such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;
14. Promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms;
15. Evolving of, and specifying, by regulations, policies and practices for Registrars, enrolling agencies and other service providers; (s) setting up facilitation centres and grievance redressal mechanism for redressal of grievances of individuals, Registrars, enrolling agencies and other service providers; (t) such other powers and functions as may be prescribed.

Chapter – V of the Act deals with Grants, Accounts and Audit and Annual Report.

Security and confidentiality of information

Security and confidentiality of information is an important aspect of the entire Act. On protection of Information, Section 28 (1) provides that states that the UIDAI must ensure the security of identity information and authentication records. Under Section 30, Biometric information deemed to be sensitive personal information. The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be “electronic record” and “sensitive personal data or information”, and the provisions contained in the Information Technology Act, 2000 and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act. Alteration of demographic information or biometric information is permissible under Section 31.

Every Aadhaar holder shall have access to own information and records of requests for authentication. The authentication records has been as "record of the time of authentication and identity of the requesting entity and the response provided" in Section 2 (d). The Section 32 states that the UIDAI must maintain the authentication records for the specified period. The Aadhaar number holder may access his authentication records subject to regulation. The UIDAI is not required to maintain the record of the purpose of authentication.

A limitation on disclosure of information is provided under Section 33. The Section 33 (1) states that a District Judge or higher court may force the UIDAI to reveal a person's identity information, i.e. Aadhaar number, photograph and demographic information, and authentication records, but not the core biometric information. The Section 33 (2) states that an official with the rank of Joint Secretary or higher may access a person's identity information including core biometric information, if the official has an order issued in the interest of national security by the Central Government.

**OFFENCES AND PENALTIES UNDER THE ACT**

Chapter VII deals with offences and penalties under the Act. Penalty for impersonation at time of enrollment – Section 34 - Whoever impersonates or attempts to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or with both. Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information – Section 35 - Whoever, with the intention of causing harm or mischief to an Aadhaar number holder, or with the intention of appropriating the identity of an Aadhaar number holder changes or attempts to change any demographic information or biometric information of an Aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which may extend to ten thousand rupees. Section 36 provides penalty for impersonation which is punishable for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Section 37 deals with Penalty for disclosing identity information - Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrollment or authentication to any person not authorized under this Act or regulations made there under or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

Penalty for unauthorized access to the Central Identities Data Repository has been provided under Section 38 of the Act. Section 39 provides Penalty for tampering with data in Central Identities Data Repository, Section 40 Penalty for unauthorized use by requesting entity, Section 41 Penalty for noncompliance with intimation requirements and Section 42 deals with General penalty. Offences by companies are also liable under Section 43 of the Act.

Section 50 empowers the Central Government’s power to issue directions. Section 50 (1) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act be bound by such directions on questions of policy, as the Central Government may give, in writing to it, from time to time: “Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section: Provided further that nothing in this section shall empower the Central Government to issue directions pertaining to technical or administrative matters undertaken by the Authority”. (2) The decision of the Central Government, whether a question is one of policy or not, shall be final.

**SUPREME COURT VERDICTS ON SCOPE AND APPLICATION OF UID ACT**

Aadhaar is the subject of several Rulings by the Supreme Court of India. On 23

September 2013 the Supreme Court issued an interim order saying that "no person should suffer for not getting Aadhaar", adding that the Government cannot deny a service to a resident who does not possess Aadhaar, as it is voluntary and not mandatory[[5]](#footnote-5).

The Court also limited the scope of the program and reaffirmed the voluntary nature of the identity number in other rulings[[6]](#footnote-6). On 24 August 2017 the Indian Supreme Court delivered a landmark verdict affirming the right to privacy as a fundamental right, overruling previous judgments on the issue. As of November 2017 a Five-Judge Constitutional Bench of the Supreme Court is yet to hear various cases relating to the validity of Aadhaar on various grounds including privacy, surveillance, and exclusion from welfare benefits. On 9 January 2017 the five-judge Constitution bench of the Supreme Court of India reserved its judgment on the interim relief sought by petitions to extend the deadline making Aadhaar mandatory for everything from bank accounts to mobile services. The Court said that the final hearing for the extension of Aadhaar Linking Deadlines will start on 17 January 2018[[7]](#footnote-7). Some civil liberty groups such as the Citizens Forum for Civil Liberties and the Indian Social Action Forum (INSAF) have also opposed the project over privacy concerns.

Further, a nine-judge Bench of the Supreme Court of India in its is rare and unanimous decision which is historic not only because it has ruled that privacy is a fundamental right, but also because it has deepened our understanding of fundamental rights as inalienable inherent rights in every human-being. Portions of the judgment that deal with data protection and privacy say that any collection of personal information that would impact privacy must have a law to back it. A corollary to this proposition is that all actions of the Unique Identification Authority of India (UIDAI) prior to the coming into force of the 2016 Aadhaar Act is of suspect constitutionality. A further question arises on what can be done about such data that was collected without a legal basis. The decision has been widely celebrated by Aadhaar’s opponents, who believe that the program is in conflict with the newly enshrined right.

Moreover, a Bench of 9-Judges has been constituted to look into questions relating to basic human rights. A 3-Judge Bench of this Court was dealing with a scheme propounded by the Government of India popularly known as the Aadhar card scheme. Under the said scheme, the Government of India collects and compiles both demographic and biometric data of the residents of this country to be used for various purposes. One of the grounds of attack on the said scheme is that the very collection of such data is violative of the “Right to Privacy[[8]](#footnote-8)”.

In spite of the fact that the validity of Aadhaar being challenged in the court, the Central Government has pushed citizens to link their Aadhaar numbers with a host of services, including mobile SIM cards, bank accounts, the Employee Provident Fund, and a large number of welfare schemes including but not limited to the Mahatma Gandhi National Rural Employment Guarantee Act, the Public Distribution System, and Old Age Pensions. Recent reports suggest that HIV patients have been forced to discontinue treatment for fear of identity breach as access to the treatment has become contingent on producing Aadhaar. It shows that the Government will continue to collect the identity and personal information particulars of the citizens of the country and to store them in a database.

The citizens are witnessing the instances that investigation agencies are securing the biometric data stored in the said data banks and using them against the individual, whose data was secured. Irrespective of the legality of procedure to secure it and produce before court of law, for admission of biometric evidence, courts are required to rely on the expert evidence. Hence, the evidentiary value of the expert evidence or opinion, before proceeding further.

Principles of Admitting Scientific Evidence

**UNITED STATES (US) COURTS**

A revolution has taken place in the last decade for the admissibility of scientific evidence in federal courts. Frye v. United States15 was the first important judgment in America regarding the admissibility of scientific evidence. The Frye test had two aspects.

Firstly, the principle or scientific technique and secondly, the acceptance.

The aspects of the test were criticized on two different grounds.

i) That there will have to be a considerable time lag for the scientific method to be accepted by the community, ii) More faith is reposed on the scientific community than in the Court of Law.

Hence, the Federal Rules Of Evidence was enacted in 1975. Rule 702, of which stated that : “If scientific, technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training or education may testify thereto in the form of an opinion or otherwise[[9]](#footnote-9) But the enactment did not settle the dispute as it neither included the Frye standard nor made a mention of the general acceptance standard. So, the United States Supreme Court laid down the guidelines in the remarkable judgment of Inc[[10]](#footnote-10). The court concluded by saying that the Federal Rules of Evidence superseded the Frye Rule and that the rigid general acceptance rule should not conquer the way of a reasonable minority scientific opinion in the form of new and emerging research based on reliable studies. It also laid down factors for the basis of scientific evidence which are also known as The Daubert Guidelines.

**The Guidelines are as follows:**

1. The content of the scientific testimony which has already been tested, can be tested using the scientific method;
2. The technique has been subject to peer review, preferably in the form of publication in peer review literature;
3. There are consistently and reliably applied professional standards and known or potential error rates for the technique.
4. Considers general acceptance within the relevant scientific community.

Later the *Kumho Tire Case*[[11]](#footnote-11), expanded the Daubert Analysis, to technical and specialized subjects that do not fall within the category of “science” After the Daubert Guidelines were framed, the Federal Rules Of Evidence were then amended in the year 2000. The Rule 702 now provides: that scientific, technical or specialized evidence (i.e.

“Expert testimony”) may be admitted if:

1. the expert is qualified;
2. the expert’s testimony will help the jury to decide issues in the case or understand the evidence; and
3. the expert’s testimony is based on sufficient facts or data; is the product of reliable methods and principles, and if the expert reliably has applied the methods and principles to the facts of the case in trial[[12]](#footnote-12)

As a result of this revolution, federal trial judges are now required to perform as so-called “gatekeepers” to determine at the threshold whether expert testimony will be allowed to be heard by the jury in civil and criminal trials before it helps the jury to decide issues in the case or understand the evidence according to Rule 702 of Federal Rules Of Evidence. In Daubert, Justice Blackmun, writing for the majority, expressed the Court’s confidence in the ability of federal trial judges to function as gatekeepers of admissibility of scientific and technical evidence to insure that only qualified experts are permitted to testify on these subjects, based on sufficient facts or data, and reliable methodology that properly has been applied to the facts of the particular case. He said: “Faced with proffer of expert scientific testimony, then, the trial judge must determine at the outset, pursuant to Rule 104(a), whether the expert is proposing to testify to

1. scientific knowledge that
2. will assist the trier of fact to understand or determine a fact in issue.

This entails preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and whether that reasoning or methodology properly can be applied to the facts in issue. We are confident that federal judges possess the capacity to undertake this review[[13]](#footnote-13). In the Joiner Case[[14]](#footnote-14) which discussed about the admissibility of scientific evidence, Associate Justice Stephen Breyer, has offered the following observation on the role of science in court cases: “In this age of science, science should expect to find a warm welcome, perhaps a permanent home, in our courtrooms. The reason is a simple one. The legal disputes before us increasingly involve the principles and tools of science. Proper resolution of those disputes matters not just to the litigants, but also to the general public – those who live in our technologically complex society and whom the law must serve. Our decisions should reflect a proper scientific and technical understanding so that the law can respond to the needs of the public”[[15]](#footnote-15). Justice Breyer, also noted that federal judges typically are generalists, not specialists and few are having training or experience in science and technology[[16]](#footnote-16). Chief Justice Rehnquist, in his opinion concurring in part and also dissenting in part from the majority opinion, was not less confident about the ability of the federal trial judiciary, but was less certain that the Court’s ruling would provide them with the means to the job assigned. He observed: “The Court speaks of its confidence that federal judges can make a ‘preliminary’ assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue. The Court then states that a ‘key question’ to be answered in deciding whether something is ‘scientific knowledge’ ‘will be whether it can be (and has been) tested.’

**UNITED KINGDOM(UK/EU)**

In England, the law dealing with the admissibility of scientific evidence is totally different from United States. The English precedential analysis shows that judges are reluctant to impose any stringent standards like ‘reliability’ test in U.S. The English courts are still following the traditional common law test “helpfulness” developed by Lawton, L.J. in the famous case R. v. Turner. The four requirements of admissibility of expert opinion in England and Wales (common law) countries are i) assistance, ii) relevant expertise, iii) impartiality and iv) evidentiary reliability.

**Assistance**

The meaning of “Assistance” was explained by the leading case of Turner that an opinion of expert “is admissible to furnish the court with ... information which is likely to be outside the experience and knowledge of a judge or jury. If on the proven facts a judge or jury can form their own conclusions without help, then an opinion of an expert is unnecessary”. In other words if the opinion of the expert is unnecessary, it becomes inadmissible. Further, the person claiming expertise must be an expert in the relevant field. Moreover, the evidence that is presented by the expert should be unbiased and purposive evidence. Finally, the expert opinion evidence must in other respects satisfy a threshold (entry) of acceptable reliability.

**POSITION IN INDIA**

In India the principles of admissibility of evidence is relevancy. According to the Indian Evidence Act, 1872, section 45 of, deals with expert evidence. The principles of admissibility in Indian Courts are that evidence can be given only of relevant facts and facts in issue. A fact may be relevant but not admissible, like in case of documentary evidence, only under certain circumstances secondary evidence of a document can be produced. If it does not satisfy the legislative provision, although a document might be relevant but it would not be admissible. It might also happen that a document or an expert report might be admissible as it is an original one or otherwise but since it is not relevant, such evidence is not accepted by courts. Therefore, in India, the principle for accepting forensic evidence is relevancy and admissibility. Under, the broad principles of ‘relevancy’ comes reliability, helpfulness, fitness which are treated as separate grounds in US. Assistance, relevant expertise, impartiality and evidentiary reliability which are the principles for admission of expert evidence in UK, also comes under the requirement of ‘relevancy’.

In India, the law regarding expert evidence is guided by sections 45 to 51 of the Indian Evidence Act, 1872. In the case of *Mahmood v. State of U.P*[[17]](#footnote-17). , the Supreme Court has defined the term expert and said that it would be highly unsafe to convict a person on the sole testimony of an expert. Although conviction based on expert evidence is unsafe, yet the incorporation of Section 53 and 53A of the Code of Criminal Procedure, 1973, mandates that in certain cases the expert evidence is indispensable. In the case of *Selvi v.State of Karnataka*[[18]](#footnote-18) the Supreme Court held that compulsory administration of forensic techniques like polygraphy, Narco-analysis and Brain-Mapping is unconstitutional if performed without the consent of the accused as it violates Article 20(3) and Article 21 of the Constitution of India[[19]](#footnote-19).

As a general rule, the opinions, inferences, beliefs and mere speculations of witnesses are inadmissible before a Court of law. It means that such types of evidence do not merit consideration. Hence they are excluded as inadmissible in the law of Evidence. Witnesses considered as fact reporting agents of the legal machinery and their role in the adjudicating process is to inform the court of facts. 'Facts' means and contain only facts and not opinions or inferences.

In the law of evidence, 'opinion' means any inference from observed facts'- However, in some situations it will be difficult to distinguish between fact and opinion because there are borderline cases in which the evidence of fact is mingled with evidence of opinion. For example, statements relating to the speed of a particular thing, identity of persons etc. are mingled with fact and inference. In such cases, the law permits witnesses to state their opinion, without which the fact finder cannot come to a correct conclusion. In some other cases, the line, which differentiates facts from opinion, may be delicate. Ordinary lay witness cannot identify certain facts with his prudence.. Such facts may be obscure or invisible to him. But a witness having a particular skill or training may be able to perceive such facts.

In India, there is no separate provision in the Indian Evidence Act regarding the admissibility of lay opinion testimony In order to admit a particular piece of opinion, it should come under Section 45 of the Act. But from the language of Section 47 to 50, lay opinion testimony relating to handwriting, existence of right or custom. usages, tenets and relationship may be admitted. In all other cases, it should satisfy the requirements under Section 45. Section 45 specifically provides that in order to admit a particular piece of opinion, the person stating that opinion must prove that he is an Expert. Sec.47 of Evidence Act reads as follows:

“When the court has to form an opin1on as to the person by whom any document was written or signed, the opinion of any person acquainted with the handwriting of the person by whom it is supposed to be written or signed that it was or was not written or signed by that person, is a relevant fact.”

From the construction of the provision itself, it is clear that "any person" may give testimony regarding the handwriting or signature and it is not restricted to experts.

One feature of this Section distinct from United States law is that it is not necessary to have direct knowledge

While interpreting the above provisions, Hon'ble Patna High Court in *Basudeo Gir v. State*[[20]](#footnote-20)87 , when the only evidence against the accused was the sole testimony of Ramkishun Ram and a footprint found in his house on a gramophone record. The said print was photographed and sent to a foot print expert along with the print took from the accused in triplicate. The question before the court was whether footprint evidence could be made admissible under Section 45 of the Indian Evidence Act Giving a liberal interpretation to Section45, the court, referred to the word "Science" as defined in the Universal Dictionary of English Language as proficiency, dexterity, skill based on long experience and practice and came to the conclusion that it was sufficiently wide enough to include the evidence of foot print expert 88 Analyzing Section 45 he said that the very amendment made out in Section 45 to include finger impression showed that it was the policy of the legislature to take the merit of developments in science.

From this case it is clear that in India, the words 'Science' and 'art' can be interpreted liberally to include all relevant changes in the society and technology. The only limitation is that, in each case the new subject of testimony should come under 'science' or 'art' If it is out side of these two subjects, court cannot include it in the list of subjects provided in Section 45.

Yet in another decision, In *State v. S.J. Chaudhary'*", Supreme Court made an attempt to state the scope and ambit of Section 45, while deciding the important question of law, whether opinion of typewriter expert is admissible under Section 45 of the Indian Evidence Act. In this case the prosecution wanted to adduce certain incriminating facts against the respondent with the help of a typewriter expert. J. S. Verma J., held, the words science and art provided in Section 45 of the Indian

Evidence Act is of wide import to include each branch of the subjects. The significance of this case was that, court imported the terms 'skill' or 'technique' with the word science, but court was silent about its application in future cases.

More over, the Law Commission of India in its 185th report of the amendment to the Evidence Act has recommended sweeping change to Section 45. After considering the English law from the commentaries of Phipson, the Commission recommended to incorporate three additional words, "trade, technical terms and identity of persons or animals" to Section 45.

The analysis of these judicial pronouncements would not only give us an acceptable definition of an expert but would also help to identify the role of an expert and scope of his evidence.

For admitting the expert evidence, the following grounds shall be considered.

1. Expert evidence should be independent and not influenced by the exigencies of litigation:
2. Expert opinion should be unbiased and objective; an expert witness should never assume the role of an advocate;
3. Facts or assumptions upon which the opinion was based should be stated, together with material facts which could detract from the concluded opinion,
4. An expert witness should make it clear when a question or issue fell outside his experience;
5. If there was insufficient data upon which to reach an opinion, this had to be stated with an indication that the opinion was provisional and any doubts had to be stated;
6. If the expert changed his mind, this had to be made known to the other side without delay:
7. There ought to be full disclosure of documents referred to in the expert evidence.

In India the term 'expert' or 'expert opinion' is not directly defined any where in the Indian Evidence Act or in any other Statute. Section 45 of the Indian Evidence Act simply says that the persons who are specially skilled in foreign law, science, art, handwriting or finger impressions are called experts Thus Section 45 limits the subject of expert testimony as stated.

**PROTECTION OF AND IMPLICATIONS OF BIOMETRIC DATA UNDER UID ACT**

Biometric information collected by the Aadhaar project could also be protected by an appropriate data protection regime, an emerging field of law which has yet to receive judicial attention despite Justice Ajit Prakash Shah’s well-publicised data protection principles[[21]](#footnote-21). India issued very basic data protection rules in+ 2011 which were widely panned for their shoddy drafting and flimsy safeguards. But because the rules only apply to bodies corporate, the UIDAI escapes regulation since it is an executive authority. Important executive summary on data protection deals:

1. With the initiation of national programmes like Unique Identification number, NATGRID, CCTNS, RSYB, DNA profiling, Reproductive Rights of Women, Privileged communications and brain mapping, most of which will be implemented through ICT platforms, and increased collection of citizen information by the government, concerns have emerged on their impact on the privacy of persons. Information is, for instance, beginning to be collected on a regular basis through statutory requirements and through egovernance projects. This information ranges from data related to: health, travel, taxes, religion, education, financial status, employment, disability, living situation, welfare status, citizenship status, marriage status, crime record etc. At the moment there is no overarching policy speaking to the collection of information by the government. This has led to ambiguity over who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the right to privacy will be protected The extent of personal information being held by various service providers, and especially the enhanced potential for convergence that digitization carries with it is a matter that raises issues about privacy.

The report proposes five salient features of framework:

1. Technological Neutrality and Interoperability with International Standards
2. Multi-Dimensional Privacy
3. Horizontal Applicability
4. Conformity with Privacy Principles and
5. Co-Regulatory Enforcement Regime

Today in India, In India, currently there are at least eighteen documents that are recognized as acceptable proofs of identity. These include passport, PAN card, ration/ PDS photo card, voter id, driving license, government photo id cards, NREGS job card, photo id issued by a recognized educational institution, arms license, photo bank ATM card, photo credit card, pensioner photo card, freedom fighter photo card, kissan photo passbook, CGHS / ECHS photo card, address card having name and photo issued by department of posts and certificate of identify having photo issued by group a gazetted officer on letterhead, disability ID Card/handicapped medical certificate issued by the respective State/Union Territories. Each of these identities serves a specific function, and none act as one comprehensive national identifier. Government issued identification is essential to the effective functioning of a State, and to the mobility of individuals in the formal structures of a country. Governments use identification to assess populations for the delivery of services, and to monitor populations within its borders. It shows the collection of personal and biometric data of citizens through one or the other mode. Biometric Identification - Issues and Challenges

Using biometric technology to identify and monitor people raises issues relating human rights and its concerns. The biometric technology in particular and often associated with intrusions into privacy of individuals. The personal and permanent natures of the physiological features of person are analyzed by a biometric system raising an inherent tension with privacy interests. When biometrics is applied in a surveillance context, concerns for privacy naturally increase as biometrics refers to a process of recording, measuring, and analyzing a range of human physiological features. The scope of features to which biometrics may be directed is all encompassing, and includes appearance, behaviour, and cognitive state of which certain physiological features are permanent, unique, and universal.

In the modern world, the biometric technologies are increasingly being used for surveillance purposes by almost all governments. For instance, in the United States military and intelligence agencies have increasingly implemented biometric technologies in their intelligence, surveillance, and reconnaissance (ISR) activities. Biometric technology is acquiring an increasingly important position in U.S. military and national security policy[[22]](#footnote-22). Biometrics have expanded in complexity and usage since 9/11, extending to logical and physical access systems; surveillance operations to fight against fraud and organized crime; immigration control and border security systems; national identity programs; identity management systems; and the determination of friend or foe in military installations[[23]](#footnote-23).

**BIOMETRIC IDENTIFICATION AND IMMUNITY AGAINST SELF-INCRIMINATION IN INDIA**

The constitution of India guarantees under Article 20(3) is a protective umbrella against testimonial compulsion for people who are accused of an offence and are compelled to be a witness against themselves. The provision borrowed from the Fifth Amendmentof the American Constitution which lays down that*,* “No person shall be compelled in any criminal case to be a witness against himself*”,* same as mentioned in the Constitution of India embodying the principles of both English and American Jurisprudence. This libertarian provision can be connected to an essential feature of the Indian Penal Code based on the lines of Common Law that, “an accused is innocent until proven guilty*”* and the burden is on the prosecution to establish the guilt of the accused; and that the accused has a right to remain silent which is subject to his much broader right, against self-incrimination. Such protection is also accorded by the provisions of The Indian Evidence Act.

The pillars of Article 20(3) is “The exercise of the power to extract answers begets a forgetfulness of the just limitations of that power[[24]](#footnote-24).” This protection is available to every person including not only individuals but also companies and incorporated bodies. This clause gives protection only if the following ingredients are present: 1. It is a protection available to a person accused of an offence;

1. It is a protection against compulsion to be a witness against oneself; and
2. It is a protection against such “Compulsion” as resulting in his giving evidence against himself.
3. It is only on making of such formal accusation that Clause (3) of Article 20 becomes operative covering that person with its protective umbrella against testimonial compulsion. It is imperative to note that, “a person cannot claim the protection if at the time he made the statement, he was not an accused but becomes an accused thereafter.” Article 20 (3) does not apply to departmental inquiries into allegations against a government servant, since there is no accusation of any offence within the meaning of Article 20 (3).

In this context, self-incrimination has been extensively discussed in Indian case in the case of Nandini Satpathy v. P.L Dani[[25]](#footnote-25). In this case, the appellant, a former Chief Minister of Orissa was directed to appear at Vigilance Police Station, for being examined in connection to a case registered against her under the Prevention of Corruption Act, 1947 and under Sections 161 and 165 and 120-B and 109 of The Indian Penal Code, 1860. Based on this an investigation was started against her and she was interrogated with long list of questions given to her in writing. She denied to answer and claimed protection under Article 20(3). The Supreme Court ruled that the objective of Article 20(3) is to protect the accused from unnecessary police harassment and hence it extends to the stage of police investigation apart from the trial procedure. However, protection under Article 20(3) is available only against compulsion of the accused to give evidence against himself. Thus, if the accused voluntarily makes an oral statement or voluntarily produces documentary evidence, incriminatory in nature, Article 20(3) would not be attracted. The term compulsion under Article 20(3) means *‘duress’*. Thus, compulsion may take many forms. If an accused is beaten, starved, tortured, harassed etc. to extract a confession out of him/her then protection under Article 20(3) can be sought.

The development and optimum utilisation, reliance on biometric evidence in the recent times in law makes the issue controversy. The issue of involuntary administration of certain scientific techniques, like narco-analysis tests, polygraph examination, etc. for the purpose of improving investigation efforts in criminal cases has gained a lot of attention. For a long time, there was a debate about whether such tests were violative of Article 20(3) or not.

In *Selvi v. State of Karnataka*[[26]](#footnote-26) the issue were brought to the Supreme Court in the through the Hon’ble Chief Justice, Justice K.G Balakrishnan spoke of behalf of the Court, and drew the following conclusions:

1. The right against self-incrimination and personal liberty are non-derogable rights, their enforcement therefore is not suspended even during emergency.
2. The right of police to investigate an offence and examine any person do not and cannot override constitutional protection in Article 20(3);
3. The protection is available not only at the stage of trial but also at the stage of investigation;
4. That the right protects persons who have been formally accused, suspects and even witnesses who apprehend to make any statements which could expose them to criminal charges or further investigation;
5. The law confers on ‘any person’ who is examined during an investigation, an effective choice between speaking and remaining silent. This implies that it is for the person being examined to decide whether the answer to a particular question would be inculpatory or exculpatory;
6. Article 20(3) cannot be invoked by witnesses during proceedings that cannot be characterised as criminal proceedings;
7. Compulsory narco-analysis test amounts to ‘testimonial compulsion’ and attracts protection under Article 20(3);
8. Conducting DNA profiling is not a testimonial act, and hence protection cannot be granted under Article 20(3);
9. That acts such as compulsory obtaining signatures and handwriting samples are testimonial in nature, they are not incriminating by themselves if they are used for the purpose of identification or corroboration;
10. That subjecting a person to polygraph test or narco-analysis test without his consent amounts to forcible interference with a person’s mental processes and hence violates the right to privacy for which protection can be sought under Article 20(3);
11. That the courts cannot permit involuntary administration of narco-tests, unless it is necessary under public interest.

Thus, according to the Supreme Court fingerprinting and other physical evidence is not covered by article 20(3). In the case of *State of Bombay v. Kathi Kalu Ogha*d[[27]](#footnote-27), the courts answered the question of whether or not the freedom against self-incrimination guaranteed under article 20(3) of the Constitution of India, which is meant to protect a person from torture from the police a question as to whether it can be extended to the collection of DNA. The courts answered this question by upholding that:

“To be a witness may be equivalent to ‘furnishing evidence’ in the sense of making oral or written statement, but not in the larger sense of the expression so as to include giving of thumb impression or impression of palm or foot or fingers or specimen writing or exposing a part of the body by an accused person for purposes of identification[[28]](#footnote-28)”

Here comes the importance of personal identification and authorisation which in general may be in the form of signatures, digital as well as biometric forms of identification (fingerprints, DNA, retina scans), security experts make a basic distinction between authentication and authorization. Authentication refers to the practices that establish that some person is who they say they are. Authorization, in contrast, deals with the policies that either grant or deny certain privileges to that person. Authentication says nothing about authorization, and vice versa; they are discrete and independent properties.

An analysis of Article 20 (3) invokes protection against self-incrimination and gives an accused the right to remain silent over any issue which tends to incriminate him. This protection by the Indian Constitution is also extended to suspects. Article 20 (3) has been carefully crafted to protect the accused from further self-incriminating himself only if any statement of his might result in prosecution. For the benefit of the Courts, the Supreme Court has distinguished between the terms “witness” and “furnish evidence”, the former including furnishing statements from one’s own knowledge and the latter referring to simply presenting documents required by the court under which protection under Article 20(3) cannot be sought.

On a close discussion of both right against self-incrimination and right to privacy, it was in *Selvi v. State of Karnataka*,[[29]](#footnote-29), this Court went into an in depth analysis of the right in the context of lie detector tests used to detect alleged criminals. A number of judgments of this Court were examined and this Court, recognizing the difference between privacy in a physical sense and the privacy of one’s mental processes, held that both received constitutional protection. This was stated in the following words:

Para 224. “Moreover, a distinction must be made between the character of restraints placed on the right to privacy. While the ordinary exercise of police powers contemplates restraints of a physical nature such as the extraction of bodily substances and the use of reasonable force for subjecting a person to a medical examination, it is not viable to extend these police powers to the forcible extraction of testimonial responses. In conceptualising the “right to privacy” we must highlight the distinction between privacy in a physical sense and the privacy of one’s mental processes.

Para 225. So far, the judicial understanding of privacy in our country has mostly stressed on the protection of the body and physical spaces from intrusive actions by the State. While the scheme of criminal procedure as well as evidence law mandates interference with physical privacy through statutory provisions that enable arrest, detention, search and seizure among others, the same cannot be the basis for compelling a person “to impart personal knowledge about a relevant fact”. The theory of interrelationship of rights mandates that the right against self-incrimination should also be read as a component of “personal liberty” under Article 21. Hence, our understanding of the “right to privacy” should account for its intersection with Article 20(3). Furthermore, the “rule against involuntary confessions” as embodied in Sections 24, 25, 26 and 27 of the Evidence Act, 1872 seeks to serve both the objectives of reliability as well as voluntariness of testimony given in a custodial setting. A conjunctive reading of Articles 20(3) and 21 of the Constitution along with the principles of evidence law leads us to a clear answer. We must recognise the importance of personal autonomy in aspects such as the choice between remaining silent and speaking. An individual’s decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy, especially in circumstances where the person faces exposure to criminal charges or penalties[[30]](#footnote-30).”

In another recent case, the Supreme Court passed an ad-interim order in Unique Identification Authority of India and anr. v. Central Bureau of Investigation[[31]](#footnote-31), the Supreme Court,Order dated March 24, 2014 where it held that the Unique Identification Authority of India was restrained from transferring anyone’s biometric information with an Aadhaar number to any other agency without such person’s consent in writing. The facts of the instant case being that the writ before the Bombay High Court sought to challenge the order of the magistrate of October 22, 2013 in which certain data of persons holding Aadhar cards had been provided to the Central Bureau of Investigation (CBI) upon CBI’s request for data under Section 91 of the Criminal Procedure Code, 1973, i.e., power to seek summons for production of a document from a person in possession of such document. The CBI had approached the magistrate in respect of a rape case of a seven year old child, which had taken place in a school washroom and the CBI had been unable to identify the offender.

The CBI had however been able to retrieve some fingerprints from the place of the incident which could help them trace the accused. hese fingerprints had been sent to the Unique Identification Authority of India (“UIDAI”) and the CBI sought information from the authority to search through its database and help identify if the fingerprints could be traced to anyone in the database. UIDAI refused to provide this information on the grounds that this would violate the privacy of Aadhar card holders. UIDAI relied on the case of *District Registrar and Collector v. Canara Bank*[[32]](#footnote-32) in which the Supreme Court had laid down the parameters of reasonable searches and seizures to ensure that a party’s fundamental right against self-incrimination is not violated under Article 20 (3) of the Constitution of India.

During arguments, UIDAI also informed the High Court that several petitions were pending before the Supreme Court with respect to data held by the UIDAI including Writ Petition No. 494/2012: Justice *K. S. Puttaswamy v. Union of India*, Writ Petition Writ Petition (Civil) No. 494/2012: Justice *K. S. Puttaswamy v. Union of India* before the Supreme Court of India. In the case before the Bombay High Court, the CBI had asked for all the data available in the State and thereafter the request was restricted to three specific persons. UIDAI refused to provide this information and then the CBI sent a CD to the UIDAI with fingerprints it had retrieved and asked UIDAI to compare them with the biometric available with it. UIDAI claimed that it did not have the requisite technology to parse through all the biometric information it held to run the comparison process. In the subsequent developments, the Supreme Court has restrained the UIDAI from sharing any biometric information in its database without the consent of the owner of such data in writing.

**BIOMETRIC IDENTIFICATION AND RIGHT TO PRIVACY IN INDIA**

The collection and use of biometrics for identification of criminals legally began in India during the 1920's with the approval of the Identification of Prisoners Bill 1920[[33]](#footnote-33). The object of the Bill is to “provide legal authority for the taking of measurements of finger impression, foot-prints, and photographs of persons convicted or arrested…”[[34]](#footnote-34)

The Bill is still enforced in India, and in October 2010 was amended by the State Government of Tamil Nadu to include “blood samples” as a type of forensic evidence[[35]](#footnote-35). Other Indian legislation pertaining to forensic evidence is the Cr.P.C. and the Indian Evidence Act. In 2005 section 53-A of the Cr.P.C. was amended to authorize investigating officers to collect DNA samples with the help of a registered medical practitioner, but the Indian Evidence Act fails to manage science and technology issues effectively[[36]](#footnote-36). The present states of statutes for DNA collection in India are not sufficient as the neglect to lay out precise procedures for collection, processing, storage, and dissemination of DNA samples.

The Code of Criminal Procedure and the Indian Evidence Act were enacted at a time when modern scientific advancement and DNA tests were not even in the contemplation of Parliament or legislature. Worldwide, it has been proven that the results of DNA tests test, if conducted in conformity with modern and latest protocol on the subject, are scientifically accurate.

Section 53 of the Code of Criminal Procedure, 1973, authorises a police officer to get the assistance of a medical practitioner in good faith for the purpose of the investigation. But, it does not enable a complainant collect blood, semen etc for bringing criminal charges against the accused. The Cr.P.C. (Amendment) Act, 2005, has brought two new sections which authorise the investigating officer to collect DNA sample from the body of the accused and the victim with the help of medical practitioner.

The introduction of DNA technology is being perceived to pose serious challenge to some legal and functional rights of an individual such as ‘Right to privacy’ and ‘Right against Self-incrimination’. And this is the most important reason why courts sometimes are reluctant in accepting the evidence based on DNA technology. Right to Privacy has been included under right to life and personal liberty or Article 21of the Indian Constitution. Article 20(3) provides Right against Self- Incrimination which protects an accused in criminal cases from providing evidence against himself or evidence which can make him guilty.

On a discussion about the application of DNA technology in the administration of justice, there are so many implications in the use of this technology. There is no doubt this new technology can be used as an effective tool in crime detection to accelerate crime control for a better society. But at the same time we overlook the fact that it cannot be implemented in any legal system without hampering some basic human rights of an accused like right against self-incrimination, right to privacy etc44. In this connection, the view expressed by Justice R.K. Abichandani requires consideration.

“The importance of fast developing DNA technology and its impact on the rights of an individual and its societal effect have created urgent need for getting acquainted with and understanding the basic of modern genetic science for an effective role by all those who are concerned with justice delivery system. The Constitution of India by some Articles like 20(3), 51A (h) and (g) tries to uplift the genetic science. The Constitutional provisions take care of the scientific developments that may take place and may be put to use for the benefit of people. The Constitution provides efficient scales for balancing

between public and private interest and the Court have put to use its provisions for an effective social engineering to protect human rights recognized by theConstitution.[[37]](#footnote-37)”

However, the Supreme Court of India has Upheld mandatory use of biometric identification for filing taxes and tax account applications etc. India’s Supreme Court, on June 9, 2017, upheld the constitutional validity of section 139-AA of the Income Tax Act, 196146, which made the Act’s biometric-based identification project, Aadhaar, mandatory for filing income tax returns and applying for Permanent Account Numbers (PANs).

In *Binoy Viswam v. Union of India & Ors*.,[[38]](#footnote-38) the Supreme Court Upholds Law Linking Aadhaar with PAN, Income Tax Act, 1961, as amended, Section 139AA, India Income Tax PANs are account numbers issued in the form of laminated cards and used for all transactions and correspondence with the Income Tax Department. However, the Court’s ruling exempts PAN holders who are not yet enrolled in Aadhaar from the provision under section 139AA(2) of the Act, which requires PAN holders to use Aadhaar numbers, until constitutional challenges to Aadhaar have been settled.

However, The Supreme Court has yet to decide whether privacy is a fundamental right under article 21 of the Indian Constitution and whether Aadhaar violates this right for lack of adequate safeguards in the collection of identity data. he Court will also be ruling on the constitutionality of government notifications issued under the Aadhaar Act that make Aadhaar mandatory for various programmes.

On the privacy and legal frame work in India, one has to locate the Aadhaar project on a larger map of Indian privacy demands a brief exercise in taxonomy. The constitutional right to privacy has evolved in three streams. The strongest privacy stream regulates surveillance. Although the Constitution’s drafters chose not to include an explicit right against invasions of correspondence and the home, the Supreme Court has protected both. But although individual freedoms are generally secure, there is a discernible judicial trend that privileges the interests of the state. That is why the Attorney-General based his anti-privacy arguments on surveillance-related cases: so that he could exploit this accompanying narrative of the state’s superior compelling interest. However, there is a significant difference between the Aadhaar project and pre-existing law regarding bodily and biometric privacy. On the face of it, the Aadhaar project is unconnected with public health, public morality, or public safety.

On privacy of individuals in India, in 2011, the erstwhile Planning Commission constituted a group of experts to suggest the contours of future Indian privacy law. Chaired by Justice Ajit P. Shah, the highly-regarded former Chief Justice of the Delhi High Court, the group considered the implications of the Aadhaar project and proposed nine principles to inform privacy law. These are the principles of notice, informed consent and opt-out choice, collection limitation, purpose limitation, access and correction, non-disclosure, data security, openness, and accountability. They are actually data protection principles; their scope is narrower than the conceptual breadth of privacy. More than 90 percent of India’s adult population’s biometric information has already been collected and when the total enrollment is done, the government will present the Aadhaar project to the Constitution Bench as a ***fait accompli.*** Nevertheless, the Supreme Court has a unique opportunity to clarify the right to privacy, besides fixing the lack of substantive due process in the Aadhaar project.

**BIOMETRIC IDENTIFICATION – NEW CHALLENGES IN INDIA**

As of now in India there is national law that empowers the government to collect and store DNA profiles of convicts, but DNA collection and testing and is taking place in many states, for example, in Pune the army is currently considering creating DNA profiles of troops who are involved in hazardous tasks in order to help identify bodies mutilated beyond recognition. In December of this year a judge in the Supreme Court ordered DNA testing on a Congress Spokesmen to determine if his child was really his child. In the orders of the Court, it was held that a distinction has to be drawn between legitimacy and paternity of the child and Section 112 of the Indian Evidence Act, 1872 is intended to safeguard the interest of the child by securing his/her legitimacy and not to paternity. Section 112 of the Indian Evidence Act, 1872 is intended to safeguard the interest of the child by securing his/her legitimacy and not to paternity. Indian Evidence Act, 1872 is intended to safeguard the interest of the child by securing his/her legitimacy and not to paternity and that that a child has a right to know the truth of his/her origin the right of a child to know his biological roots can be enforced through reliable scientific tests and if the interest of the child is best sub-served by establishing paternity of someone who is not the husband of his mother, the Court should not shut that consideration altogether; Indian law casts an obligation upon a biological father to maintain his child and does not disregard rights of an illegitimate child to maintenance.

In N.D. Tivari paternity test case, the Supreme Court N.D. Tiwari, Congress leader and former Governor of Andhra Pradesh to provide blood samples for DNA test in the paternity test case. Justice S Rabindra Bhatt of Delhi High Court should be complimented for ordering DNA test for former Andhra Pradesh Governor N.D. Tiwari to decide paternity-claim filed by one Rohit Shekhar, whereupon the Delhi high court had said that N.D. Tiwari could be compelled to give blood sample[[39]](#footnote-39). It further said that police assistance could be sought if he refused to agree to do it voluntarily.

The introduction of the DNA Technology has posed serious challenge to some legal and fundamental rights of an individual such as ‘Right to Privacy’, ‘Right against self-incrimination’. And this is the most important reason why courts sometimes are reluctant in accepting the evidences based on DNA Technology. Right to Privacy has been included under Right to Life and Personal Liberty or Article 21 of the Indian Constitution, and Article 20(3) provides Right against Self-Incrimination which protects an accused person in criminal cases from providing evidence against himself or evidences which can make him guilty.

But it has been held by the Supreme Court on several occasions that Right to Life and Personal Liberty is not an absolute Right. In Govid Singh v. State of Madhya

Pradesh[[40]](#footnote-40), Supreme Court held that a fundamental right must be subject to restriction on the basis of compelling public interest. DNA test or ‘DNA Profiling’ as popularly known is a technique in which a sample of DNA is run through a laboratory assay to generate information about it, looking specifically for DNA which could identify the source of the sample, or be used as a base of comparison between two samples. This technique is used at various places for different purposes ranging from law enforcement to Medical Treatment.

**DNA AND FORENSIC EVIDENCE**

In the history, hardly one can find the standardized forensic practices which aided in criminal justice dispensation system and awarding punishments. The Criminal investigations and trials relied on oath, confessions whether forced or voluntary and witness testimony. However ancient sources contain several accounts of techniques that foreshadow the concepts of forensic science that is developed centuries later. The first recorded example of forensic dentistry may be the account of Agrippina, the Roman emperor Nero's mother, who sent for the head of her enemy Lollia Paulina[[41]](#footnote-41) to verify her death. In ancient China polygraph tests used to be conducted in which they relied on physiological reactions. According to recorded history, in ancient Rome, officials employed experts in handwriting analysis to compare the writing styles of scribes in order to detect forgery. In ancient India medical opinion was frequently applied to the requirements of the law. It was the law for the minimum age for girls who was fixed at 12 years and the duration of pregnancy was recognized as being between 9 and 12 lunar months with an average of 10 months and there is evidence that doctors had to opine on such case. In India, Sir William Herschel was one of the first to advocate the use of fingerprinting in the identification of criminal suspects.

Forensic evidence is a discipline that functions within the parameters of the legal system. Its purpose is to provide guidance to those conducting criminal investigation and to supply to courts accurate information upon which they can rely in resolving criminal and civil disputes. Forensic science, an amalgamation of almost all faculties of knowledge, is an essential and efficient enabler in the dispensation of justice in criminal, civil, regulatory and social contexts. It is defined as the application of science in answering questions that are of legal interest.

In the contemporary modern world, forensic science is an advanced scientific technique which is used in criminal and civil investigations and this science is capable of answering important questions and forms an integrated part of criminal justice system. The forensic evidence includes all well-known techniques such as fingerprint analysis, DNA analysis, ballistic, firearms or explosive culture etc. It helps to convict those guilty of crime as well as can exonerate the innocent. Forensic evidence often helps to establish the guilt or innocence of possible suspects. Fingerprint as a method of identification is recognized throughout the world and is accepted by the judiciary. The fingerprints as evidence are important because of the following features of the fingerprints. They are unique, they are permanent, they are universal, they are inimitable, they are classifiable, and they are frequently available in crime situations as evidence.

In India, the application of forensic science to crime investigation and trial has to stand the limitation of law. The predominant questions that arises on the sustenance of forensic evidence is depend upon at least three parameters viz. a) What is the constitutional validity of such techniques? b) To what extent does the law allow the use of forensic techniques in crime investigation? c) What is the evidentiary value of the forensic information obtained from the experts?

This issue of DNA test was discussed at length in *Gautam Kundu v. Bengal*[[42]](#footnote-42), where the division bench of apex court, inter alia, held as follows:- ― (1) That courts in India cannot order blood test as matter of course

1. There must be a strong prima facie case in that the husband must establish non access in order to dispel the presumption arising under section 112 of the

Evidence Act

1. No one can be compelled to give sample of blood for analysis.

However subsequently a full bench of the *Supreme Court in Sharda v.*

*Dharmpal*[[43]](#footnote-43), considered the power of a matrimonial court to order such test and clarified that *Goutam Kundu v. Bengal case* is not an authority for the proposition that under no circumstances the Court can direct that blood tests be conducted. It, having regard to the future of the child, has, of course, sounded a note of caution as regard mechanical passing of such order.

The introduction of the DNA technology has posed serious challenge to some legal and fundamental rights of an individual such as “Right to privacy”, “Right against Self-incrimination”. And this is the most important reason why courts sometimes are reluctant in accepting the evidence based on DNA technology. Right to Privacy has been included under Right to Life and Personal liberty or Article 21 of the Indian Constitution, and Article 20(3) provides Right against Self- Incrimination which protects an accused person in criminal cases from providing evidences against himself or evidence which can make him guilty. But it has been held by the Supreme Court on several occasions that Right to Life and Personal Liberty is not an absolute Right. Further, it is on this basis that the constitutionality of the laws affecting Right to Life and Personal Liberty are upheld by the Supreme Court which includes medical examination. However, on the basis various courts in the country have allowed DNA technology to be used in the investigation and in producing evidence. The refusal of the Supreme Court to dismiss the Delhi High court‘s decision ordering veteran congress leader N.D. Tiwari to undergo the DNA test is very important from the viewpoint of the admissibility of such evidence. In this case, Rohit Shekhar has claimed to be the biological son of N.D. Tiwari, but N.D. Tiwari is reluctant to undergo such test stating that it would be the violation of his Right to privacy and would cause him public humiliation. But Supreme Court rejected this point stating when the result of the test would not be revealed to anyone and it would under a sealed envelope, there is no point of getting humiliated. Supreme Court further stated that we want young man to get justice; he should not left without any remedy. It would be very interesting to see that how courts in India would allow the admissibility of DNA technology in the future[[44]](#footnote-44).

The Constitution of India under Articles 20(3) which is in the fundamental rights chapter of the constitution, declare that no person accused of any offence shall be compelled to be a witness against himself. Article 20(3) is based upon the presumption drawn by law that the accused person is innocent till proved guilty. Article 20 (3) of the Constitution of India guarantees fundamental right against self incrimination and guards against forcible testimony of any witness. The fundamental right guaranteed under Article 20 (3) is a protective umbrella against testimonial compulsion in respect of persons accused of an offence to be witness against themselves. The protection is available not only in respect of evidence given in a trial before Court but also at previous stage. The protection against self-incrimination envisaged in Article 20 (3) is available only when compulsion is used and not against voluntary statement, disclosure or production of document or other material. It also protects the accused by shielding him from the possible torture during investigation in police custody. Criminal law considers an accused as innocent until his guilt is established beyond reasonable doubt[[45]](#footnote-45). This right has been taken to ensure that a person is not bound to answer any question or produce any document or thing if that material would have the tendency to expose the person to conviction for a crime.

In Indian context, the call for DNA test on civil side is generally made to settle the paternity issue involved in cases of divorce, maintenance, inheritance and succession etc. It is noteworthy that Section 112 provides for the legitimacy of a child born during wedlock and the only ground to rebut this presumption is non access of the husband. Thus at one point of time it was an issue before the court dealing with paternity issues whether such test could be ordered.

At present in India there is no concrete law to govern issues of admissibility of forensic technique. Some sections i.e. Sections 53, 54, 53(A), 164(A) of Code of Criminal procedure govern science and technology issue to certain extend. As such it is completely left on judicial discretion either to permit DNA test or to deny any such request. Such a condition creates confusion and uncertainty over subordinate judiciary.

In *Asit Kapoor v. Union of India[[46]](#footnote-46),* it was held that no party to a legal proceeding can be compelled for any scientific test against his/her will as it has effect of infringing upon his right to privacy. Some important guidelines are issued in *Gautama Khandu vs. State of West Bengal & Anr*.[[47]](#footnote-47), which is summed up as follows:

* Matrimonial court has power to order a person to undergo some medical test.
* Such order wouldn‘t be considered as violation of Right to personal liberty enshrined under Article 21 of Indian Constitution.
* Such a power is exercise by court when there is strong prima facie case and sufficient material before the court. If the respondent refuses to medical examination despite of the order of the court, then court will be entitled to draw adverse inference against him.

In view of the above discussions, Indian judiciary had adopted forensic evidence but it is legislative machinery which is lagging behind in assimilating scientific development which plays important role not only to solve high profile cases but rape cases and post-conviction matter also.

The aspect of DNA and self-incrimination, a Constitution Bench of the Hon’ble Supreme Court, in *Selvi v. State of Karnataka1,* while testing the validity of DNA tests on the anvil of Article 20(3) of the Constitution of India, made following observation.

The matching of DNA samples is emerging as a vital tool for linking suspects to specific criminal acts. It may also be recalled that as per the majority decision in Kathi Kalu Oghad (AIR 1961 SC 1808), the use of material samples such as fingerprints for the purpose of comparison and identification does not amount to a testimonial act for the purpose of Article 20(3). Hence, the taking and retention of DNA samples which are in the nature of physical evidence does not face constitutional hurdles in the Indian context.

On application of DNA evidence in criminal cases, the test can be effectively used in criminal cases for the following purpose. First, it assists in positively identifying the perpetrators of crime, particularly in cases of sexual assault and homicide where identification is often a central issue, secondly, to identify the remains of victims of violent crimes. The most suitable application of DNA tests for these purposes is evident in two popular cases namely, Santosh Kumar Singh v. State, establishing commission of rape by the appellant and Surendra Koli v State of U.P. to identify dead bodies of victims.

**THE DNA TEST AND RIGHT AGAINST SELF INCRIMINATION.**

Further, Section 73 of the Indian Evidence Act4 empowers the court to direct any person including an accused to allow his finger impressions to be taken. The Supreme Court has also held that being compelled to give fingerprints does not violate the constitutional safeguards given in Article 20(3). In *The State of Bombay v. KathiKalu Oghad and Other,*, the court held that giving thumb impression, specimen signature, blood, hair, semen etc. by the accused do not amount to ‘being a witness’ within the meaning of the said Article. The accused, therefore, has no right to object to DNA examination for the purposes of investigation and trial. The Bombay High Court in a significant verdict in the case of *Ramchandra Reddy and Ors., v. State of Maharashtra*, upheld the legality of the use Brain finger-printing, lie detector test and the use of truth serum or narco-analysis. In *Dinesh Dalmia v. State*, the Madras High Court held that subjecting an accused to narco-analysis does not tantamount to testimony by compulsion. However, in a subsequent case, *Selvi & Ors v. State of Karnataka & Anr. case*, the Supreme Court questioned the legitimacy of the involuntary administration of certain scientific techniques for the purpose of improving investigation efforts in criminal cases.

In the above mentioned case, the Supreme Court held that brain mapping and polygraph tests were inconclusive and thus their compulsory usage in a criminal investigation would be unconstitutional. The Code of Criminal Procedure, 1973 was amended in 2005 to enable the collection of a host of medical details from accused persons upon their arrest. Section 53 of the Criminal Procedure Code 1976 provides that upon arrest, an accused person may be subjected to a medical examination if there are “reasonable grounds for believing” that such examination will afford evidence as to the crime. The scope of this examination was expanded in 2005 to include “the examination of blood, blood-stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case.

In *Pantangi Balarama Venkata Ganesh v. state of Andhra Pradesh*, the court held that the DNA test on identity is admissible. However, the provision inserted through an Amendment in 2005 is limited to rape cases only and this section also does not enable a complainant to collect blood, semen, etc, for bringing criminal charges against the accused; neither does it apply to complaint cases. In similar lines, Section 164A Code of Criminal Procedure, 1973 provides for the medical examination of a woman who is an alleged victim of rape within twenty four hours and such examination includes the DNA profiling of the woman. Both the sections authorize any medical practitioner within the meaning of Section 2(h) Indian Medical Council Act, 195610 to collect a DNA sample. Under Indian Evidence Act, 1872, forensic report is considered as “opinion” tendered by expert and an expert may be defined as a person who, by practice and observation, has become experienced in any science or trade. Therefore, he is one who has devoted time and study to a special branch of learning, and is thus especially skilled in that field wherein he is called to give his opinion11. The credibility of an expert witness depends on the reasons stated in support of conclusion and the tool technique and materials, which form the basis of such conclusion. However, the court is free to disagree with the conclusions drawn by the expert and rely on other evidences for the purpose of decision.

**ADMISSIBILITY OF THE DNA EVIDENCE**

The admissibility of the DNA evidence before the court always depends on its accurate and proper collection, preservation and documentation which can satisfy the court that the evidence which has been put in front it is reliable. There is no specific legislation which is present in India which can provide specific guidelines to the investigating agencies and the court, and the procedure to be adopted in the cases involving DNA as its evidence. Moreover, there is no specific provision under Indian Evidence Act, 1872 and Code of Criminal Procedure, 1973 to manage science, technology and forensic science issues. Due to lack of having any such provision, an investigating officer has to face much trouble in collecting evidences which involves modern mechanism to prove the accused person guilty. Section 53 of Code of Criminal Procedure, 1973 authorizes a police officer to get the assistance of a medical practitioner in good faith for the purpose of the investigation. But, it doesn‘t enable a complainant to collect blood, semen etc. for bringing the criminal charges against the accused. The amendment of Cr. P. C. by the Cr. P. C. (Amendment) Act, 2005 has brought two new sections which authorize the investigating officer to collect DNA sample from the body of the accused and the victim with the help of medical practitioner. These sections allow examination of person accused of rape by medical practitioner and the medical examination of the rape victim respectively. But the admissibility of these evidences has remained in a state of doubt as the opinion of the Supreme Court and various High Courts in various decisions remained conflicting. Judges do not deny the scientific accuracy and conclusiveness of DNA testing, but in some cases they do not admit these evidences on the ground of legal or constitutional prohibition and sometimes the public policy.

**AADHAR CONTROVERSY**

The discourse around Aadhaar has only aggravated since its inception, and one of the primary contentions of the debate has been lack of a statutory force behind the initiative. Amidst all the speculations, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016 was introduced on 3rd of March as a money bill, on the grounds that subsidies and other benefits will be drawn from the Consolidated Fund of India. The Bill seeks to resolve the contention of the lack of a legislation backing Aadhaar. The Bill also allows for more schemes to be attached to Aadhaar in future. Presently, there are a handful of schemes attached to the Aadhaar which have been approved by the Supreme Court. The Bill is an ambitious task to provide a framework for operationalization of Aadhaar.

Civil rights groups have opposed the Aadhaar biometric system, which is based on centralized records of all ten fingerprints and iris scans, as their extensive use allegedly encroach on the privacy rights of Indians. There is an apprehension that Aadhaar is surveillance technology masquerading as secure authentication technology. But the Government of India hold that the Aadhaar Act, passed in Parliament provides the legal backing for making the biometric identification compulsory.

After coming into force of Aadhar biometric identification as compulsory in India, there are several documents one need to link to your Aadhaar card. In order to operate transaction in the following linking certain documents with Aadhaar card has now been made compulsory by the government. These measures are being put into place to ensure that benefits from all government schemes reach the people. The process is relatively simple, and can be done both, online or offline.

The following are issues which are being discussed on the implementation of Aadhaar linkage and privacy of individuals and the Government's ambitious unique identification project, Aadhaar, has drawn flak from several sections of society. Aadhar is an important document as it is a complete residence proof and identity proof. Details in Aadhar card are easy to modify, physical possession is also not required and theirs is no chance of getting it stolen or any misuse by any other person as Aadhar card is useless without biometrics verification or One-Time-Password.

**ARGUMENTS IN FAVOUR OF AADHAAR**

1. Aadhaar would qualitatively restructure the role of the state in the social sector.
2. Aadhaar is the most widely held identity document in the country with around 92 crore people under it. Restricting Aadhar’s voluntary use would mean a majority of the population will not be able to use it to access various social schemes.
3. Aadhaar can help eliminate duplication and impersonation in muster rolls and beneficiary lists, plugging the leaks that currently characterise most social welfare initiatives.
4. It will impact nearly 1 crore workers under MGNREGA, who use Aadhaar to withdraw their wages every month, and nearly 30,00,000 pensioners.
5. Countering the privacy argument, UIDAI says the data captured is secure and encrypted right at the source and all biometrics are stored in the Government of India’s servers with “world class security standards”
6. Aadhaar number shall also help to eliminate the duplicate cards and fake cards for non-existent beneficiaries in the schemes.
7. “Aadhaar” shall be able to reduce the involvement of middlemen who siphon off part of the subsidy.

**ARGUMENTS AGAINST AADHAAR**

The opposition to Aadhaar mostly centres on the issues of surveillance and privacy. The wealth of personal information collected by the Aadhaar database could be misused are unwarranted.

The biometrics database collected by UIDAI was not secure since private agencies were involved in collecting the personal information of individuals without any supervision by the government or its pertinent wings.

By collecting personal information and biometric data, the project violated the individual’s right to privacy.

Instead of ensuring inclusion, it had become an instrument of exclusion by denying services to people who didn’t enrol for it or chose not to.

There have been instances of errors in authentication. Such errors could make Aadhaar exclusionary.

There is an ongoing debate on whether India and Indians need one number to bind them all.

Aadhaar, the technological design, is different from Aadhaar Act, the legislation, which is responsible for implementing the technology. While they are intertwined inextricably, much of the privacy and surveillance concerns stem from the Act.

As per the UIDAI website, there is no provision to opt out of Aadhaar nor is it possible to purge the citizen’s information from the database.

**THE ISSUES RAISED BY HUMAN RIGHTS ORGANISATIONS**

The arguments Aadhar making mandatory under the law, the following issues are being raised by activists who argue that such large data base is subject to many legal consequences and also data misuse.

1. For making Aadhar mandatory, critics have accused government of not initiating a fruitful and convincing discussion on whether Aadhaar should be made mandatory in India.
2. The Supreme Court of India itself asserted in 2013 that Aadhaar should be voluntary, not mandatory. The case is still pending before he apex court.
3. The biggest impact of making Aadhar mandatory will be on people who rely on food subsidies. An estimated 67 per cent of India’s population relies on the food subsidies and benefits available for cereals due to the National Food Security Act of 2013.
4. Since the Aadhar law has now struck down on violation of fundamental rights and privacy invasion, there is a danger that several government schemes might find themselves stuck, in the future.
5. Experts argue that the government’s move to make Aadhaar mandatory is a violation of the Supreme Court order. It “unfairly expands the scope of Aadhaar beyond welfare services” and “leaves citizens with no choice” but to not enrol.
6. Experts also argued that with Aadhaar being made mandatory, different databases are getting linked by a common ID, making personal information vulnerable to hacking and government surveillance. Effectively, this makes every citizen vulnerable.
7. UID doesn’t collect information on where or why Aadhaar is being used to verify identity of an Aadhaar-card holder. The UID database has no information on the reason or location of authentication. As per the UIDAI, apart from the moment of authentication, no other information is recorded.
8. Aadhaar Act, 2016 states that information will not be disclosed except “in interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government.” But there is no specific definition of ‘national security’ in the Act. The government refused to define the scope of “national security”, which means it has all the power to access someone’s data without any judicial oversight.
9. Linking Aadhaar to all government and private services gives the government access to large amount of data which it can use in the name of ‘national security’.
10. Another important hindrance is that in few cases, labourers and poor people, the primary targets of the Aadhar process, often do not have clearly defined fingerprints because of excessive manual labour. Even old people with “dry hands” have faced difficulties. Weak iris scans of people with cataract have also posed problems. In many cases, it is reported that agencies have refused to register them, defeating the very aim of inclusion of poor and marginalized people.

In the recent case[[48]](#footnote-48) on Aadhar ‘Right to Privacy is a fundamental right’ judgement by the Supreme Court, there still exists the issue of Aadhaar being valid or not which is still pending. Much controversy has lit upon the conflict of Aadhaar, specifically, The Aadhaar Act, 2016 and the Right to Privacy of every citizen of the country being violated through it. The problems with the Aadhaar Act, 2016 in concern to privacy are mainly comprised of two parts: firstly, Aadhaar Act making Aadhaar compulsory for every citizen and also making its compulsory linkage to other services, including PAN and phone numbers. It further makes an amendment to the Income Tax Act wherein for tax returns to be processed, one needs to link their Aadhaar number to their PAN. A failure to do this could also lead to invalidity of the respective PAN. These legislations are a forced compulsion for the citizens to link their Aadhaar to these documents which is a problem as Aadhaar inherently requires a lot of personal and confidential information like biometrics, fingerprints, etc. which connects to the second issue of data security. The Aadhaar Act, 2016 allows sharing of data under the Aadhaar numbers for the purposes of “national security” which a vague and undefined term. Further, Aadhaar is applicable to commercial purposes as well and has the participation of private parties in its data access which leaves the citizens a huge risk of data leak given that there are no existing privacy laws in India. The active government wants the Aadhaar policy to continue and is gradually making Aadhaar mandatory for more documents, for

e.g., driving licence, which is in plan to also be mandatorily linked to Aadhaar.

In *People’s Union for Civil Liberties v. Union of India*[[49]](#footnote-49) concerning legislation authorising telephone tapping that had been used to justify surveillance of several politicians, the Supreme Court laid down guidelines concerning how such judgments should be made when legislation concerns national security. In the 1994 case of *R. Rajagopal v State of Tamil Nadu*60, the Supreme Court directly linked the right to privacy with Article 21 of the Constitution and held that,

“the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. No one can publish anything concern the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages”.

Over the past several decades, judicial activism in India has developed precedent wherein the right to privacy has been inferred through other articles of the Constitution. On July 19, 2017 a nine judge bench of the Supreme Court, led by Chief Justice Khehar, assembled to determine whether Indian citizens have a fundamental right to privacy under our Constitution.

In the 21st century, it is rightly opined by many that a government that cannot or will not protect its citizens’ privacy rights cannot credibly maintain a democratic regime of equal treatment under the rule of law. Freedom of opinion and association; freedom of religion, the ability to make choices and decisions autonomously in society free of surrounding social pressure, including the right to vote — all of these depend on the preservation of the “private sphere.”

But, unfortunately the Government of India speaking through its AttorneyGeneral, has repeatedly declared that it is the government’s position that Indian citizens have no constitutional right of privacy. However, the pressure on the government very much increased when the Supreme Court refused simultaneous applications by multiple agencies demanding relief from the Supreme Court’s interim order limiting the use of Aadhaar pending the Court’s final decision. By referring these government applications to a constitutional bench of the court has assured Indians that a decision on their fundamental rights will not be long delayed. The Attorney-General argued that the poor, whose welfare is at stake in the continuance of subsidy payments and other benefits, must be prepared to surrender their right of privacy, if any, in order to continue receiving benefits. This argument was sharply rejected by the bench, which recognises that the poor have the same rights as the rich, and interim as well as permanently, in any democratic society. This is not that claiming, a conflict between the needs of the poor and a very few who care about everyone’s fundamental right to privacy. The government’s most basic obligation is to protect its citizens’ rights — both their right to sustenance and their right to the privacy that enables freedom — equally.

The ultimate resolution of this present controversy must recognise both the need for Aadhaar in order to provide efficient and honest government services to citizens and the need for stringent rules concerning access to and security of citizens’ biometric data, in order to preserve their privacy. The Supreme Court’s action ensured that the Union government must respond to both halves of the problem. In particular, the Indian Supreme Court is likely to find itself asking Government of India about what in Indian and U.S. law is called the “doctrine of unconstitutional conditions”. Both Supreme Courts have held that the government cannot condition receipt of public benefits on waiver of fundamental rights. This is in sharp contradiction to the argument offered in the Supreme Court this week by the counsel for Centre for Civil Society, when he told the bench that “a person who has a right to privacy should be allowed to waive it for greater benefit.” The good news is that the Supreme Court has shown it knows exactly what’s at stake. It is worthwhile to note that the Supreme Court Constitutional Bench led by the Chief Justice of India in a Writ Petition between Justice K S Puttaswamy (Retd) and another v. Union of India[[50]](#footnote-50), held that citizens cannot be forced to produce his Aadhaar to avail themselves of government welfare schemes and benefits. It had even hinted that the government risked contempt of court if it chooses to continue to make the Aadhaar number a mandatory condition.

However, On October 15, 2016, the Constitution Bench had extended the voluntary use of Aadhaar cards to the Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA), pensions schemes, Employee Provident Fund and the Prime Minister Jan Dhan Yojana. The Bench was modifying an August 2015 order restricting Aadhaar use to only PDS and LPG distribution.

The Supreme Court stated[[51]](#footnote-51) that the six schemes mentioned in the previous orders are the public distribution scheme (PDS), LPG distribution scheme, the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS), National Social Assistance Programme (Old age pensions, widow pensions, disability pensions), the Prime Minister’s Jan Dhan Yojana (PMJDY) and Employees’ Provident Fund Organisation (EPFO).

In continuation of the interim orders in Aadhaar case, On 27 March 2017, the court affirmed that Aadhaar cannot be mandatory for availing benefits under welfare schemes, though it can be mandatory for other purposes (such as income tax filings, bank accounts etc). On June 9, 2017, it partially read down Section 139AA of the Income Tax Act that mandated an individual to link their Aadhaar for filing their Income Tax Returns. On 11 August 2015, the Supreme Court had directed the government to widely publicise in print and electronic media that Aadhaar is not mandatory for any welfare scheme.

As of now there is no specific law on personal data protection. However, a draft bill which has been prepared as model by the Centre for Internet Society has tried to define what sensitive personal data is; and according to them sensitive personal data” means personal data as to the data subject’s –

1. Biometric data;
2. Deoxyribonucleic acid data;
3. Sexual preferences and practices;
4. Medical history and health;
5. Political affiliation;
6. Commission, or alleged commission, of any offence;
7. Ethnicity, religion, race or caste; and
8. Financial and credit information

The draft provides for collection of personal data with prior informed consent and also subject to certain conditions contained in the future Act to be enacted. The draft also provides for transfer of data, regulation of disclosure of personal data either with our without prior consent of the person concerned. The draft aims at constitution of Data Protection Authority with powers and functions of such authority together with conditions of service. Having passed such law, the Data Protection Authority shall be The Data Protection Authority shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974), and every proceeding before the Data Protection Authority shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860).

In view of the gravity and importance of this, the Government of India inches closer towards enacting a law for data protection, an expert committee appointed by the government of India began its public consultation process for feedback before it drafts the law. The committee of experts chaired by Justice B N Srikrishna will be holding four public consultations, starting with one in New Delhi followed by Hyderabad), Bengaluru, and Mumbai to start with. The expert committee headed by Justice Srikrishna , a former Judge of the apex court, has Department of Telecom Secretary Aruna Sundararajan, Unique Identification Authority of India head Ajay Bhushan Pandey, MeitY Additional Secretary Ajay Kumar, Indian Institute of Technology-Raipur Director Prof Rajat Moona, National Cybersecurity Coordinator Gulshan Rai, Indian Institute of Management-Indore Director Prof Rishikesha Krishnan, Vidhi Centre for Legal Policy's Arghya Sengupta and Data Security Council of India's Rama Vedashree as its members. The committee headed by Justice B N Srikrishna (retired) to look into various aspects of data protection it is expected and in accordance with the information given by the Attorney General of India to the Supreme Court[[52]](#footnote-52), the committee will finalise its report by March, 2018.

In view of the above, in the pending case before the Supreme Court on Aadhaar, the issues before apex court are:

1. Whether a citizen has a right of choice, i.e, right to refuse to give biometric data? Can state coerce a citizen to part with the personal and biometric data? Is it not violation of fundamental right of privacy under Part III (as per declaration in Puttaswamy judgment) and right against self incrimination guaranteed specifically under Article 20(3)?
2. Why a citizen should not have a right of choice to be out of Aadhaar net?
3. Is it not breach of privacy of a billion people if their name, photo, address, gender, date of birth, parent’s names, etc are exposed to and by anonymous sellers?
4. How can Centre go ahead with Aadhaar Act without having comprehensive legislation on right to privacy and reasonable restrictions on it?

However, The Data (Privacy And Protection) Bill, 2017 was introduced in Lok Sabha as Bill No. 100 of 2017 By Shri Baijayant Panda, M.P. which aims to codify and safeguard the right to privacy in the digital age and constitute a Data Privacy Authority to protect personal data and for matters connected therewith**.**

**CONCLUSION:**

To conclude the discussion on biometric identification vis-a-vis right to privacy and right against self-incrimination, the question of possible data theft and data protection of more than a billion Indians is at stake. The Supreme Court, while declaring right to privacy is a fundamental right, paused the compelling conditions of completion of linkage of Aadhaar with many activities like the banks, insurance companies, mobile operators, public services to mention a few but many more. The pertinent questions that arose with requires consideration, inter alia, legal are that whether the biometric data of a more than billion people of India are safe.

It was reported by the Tribunal on January 4, 2018 that for Rs 500-00 an access to a billion identities on UID database is possible. It was also reported that there are one lakh illegal users of UID data, including anonymous groups created on WhatsApp. Government websites and educational institutions displayed personal information along with UID numbers in November 2017. Around 36 per cent people are excluded from PDS in Rajasthan, because they could not authenticate due to finger print failures. In Jharkhand, many starved to death because they could not link UID numbers with their ration cards.

Biometrics is now as untested technology even by the UIDAI’s own admission. Critics question the imposition of such technology on entire population exposing the citizens to tracking. RTI Act mandates the state to be transparent to its people, but most of the information is denied under privacy clause, whereas the UDI allows every individual to be profiled and tracked by state and private companies.

1. Kharak Singh v. State of UP, 1 SCR 332 (1964); also see R.C. Jain, National Human Rights Commission, India, Indian Supreme Court on Right to Privacy, July, 1997. [↑](#footnote-ref-1)
2. As published in the UN, Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Third periodic reports of States parties due in 1992 Addendum -India/1, June 17, 1996. [↑](#footnote-ref-2)
3. H. Weschler, "Biometric security and privacy using smart identity management and interoperability: Validation and vulnerabilities of various techniques", Rev. Policy Res., vol. 63, pp. 64, 2012 [↑](#footnote-ref-3)
4. The Planning Commission has been changed to The National Institution for Transforming India, NITI Aayog [↑](#footnote-ref-4)
5. "Don't tie up benefits to Aadhaar, court tells Centre". The Hindu. 24 September 2013. Retrieved 157-2017.. [↑](#footnote-ref-5)
6. "Aadhaar Card Not Mandatory, Supreme Court Rules". NDTV. 11 August 2015. Retrieved 15-72017. [↑](#footnote-ref-6)
7. Government To Extend All Aadhaar Linking Deadlines To March 31". [↑](#footnote-ref-7)
8. Justice K S Puttaswamy (Retd.),and Another v. Union of India And Ors., Writ Petition (Civil) No. 494 of 2012, Judgment pronounced on 24-8-2017. [↑](#footnote-ref-8)
9. Federal Rules of Evidence 1975: Available at https://www.law.cornell.edu/rules [↑](#footnote-ref-9)
10. Daubert v.Merell Dow Pharmaceuticals, Inc 509 U.S 579 (1993) [↑](#footnote-ref-10)
11. Kumho Tire company, ltd v. Carmichael, 526 U.S 137 (1999) [↑](#footnote-ref-11)
12. Dr.MP Kantak, Dr M.S. Ghodkirekar & Dr. S.G.Pemi “Utility of Daubert guidelines in India” 26(3) JIAFM 110 (2004) [↑](#footnote-ref-12)
13. Daubert, 509 U.S. at 591 (Emphasis added) (Internal Citations Omitted) [↑](#footnote-ref-13)
14. General Electric V. Joiner, 522 U.S 136 (1997) [↑](#footnote-ref-14)
15. Stephen Breyer, Introduction to REFERENCE MANUAL ON SCIENTIFIC EVIDENCE 1, 2 (2nd

    edn.,2000) [↑](#footnote-ref-15)
16. “[M]ost judges lack the scientific training that might facilitate the evaluation of scientific claims or the evaluation of expert witnesses who make such claims. Judges typically are generalists, dealing with cases that can vary widely in subject matter.” Stephen Breyer, Introduction to REFERENCE

    MANUAL ON SCIENTIFIC EVIDENCE 1, 4 (2nd edn., 2000) [↑](#footnote-ref-16)
17. AIR 1976 SC 69 [↑](#footnote-ref-17)
18. 2010 (7) SCC 263 [↑](#footnote-ref-18)
19. Article 20(3) Prohibits self-incrimination and Article 21 guarantees Right to life and personal liberty. [↑](#footnote-ref-19)
20. AIR 1959 Pat 534 [↑](#footnote-ref-20)
21. Report of the Group of Experts on Privacy, Planning Commission , Government of India, 2012 [↑](#footnote-ref-21)
22. Department of Defence, “Project Management Department of Defense Biometrics,” Program Executive Office: Intelligence Electronic Warfare & Sensors; https://peoiews.army.mil/programs/ biometrics, accessed July 2017. [↑](#footnote-ref-22)
23. N. Evans, S. Marcel, A. Ross, and A. Beng Jin Teoh, “Biometrics security and privacy protection,” IEEE Signal Processing Mag., vol. 17, 2015.

    [↑](#footnote-ref-23)
24. Wigmore, Evidence, 2264 (2nd edn, 1923) as cited in Fred Inbau, Self-Incrimination: what can a Accused Person be compelled to do?, 28(2) Journal Of Criminal Law And Criminology 261, 264 (1937). [↑](#footnote-ref-24)
25. Nandini Satpathy v. P.L Dani, AIR 1978 SC 1025 [↑](#footnote-ref-25)
26. Selvi v. State of Karnataka, AIR 2010 SC 1974. [↑](#footnote-ref-26)
27. Ibid supra [↑](#footnote-ref-27)
28. AIR 1961 SC 1808 [↑](#footnote-ref-28)
29. Selvi v. State of Karnataka, (2010) 7 SCC 263 [↑](#footnote-ref-29)
30. Supra note no 33. [↑](#footnote-ref-30)
31. Unique Identification Authority of India and Anr. v. Central Bureau of Investigation, Special Leave to Appeal (Crl) No (s).2524/2014 [↑](#footnote-ref-31)
32. Appeal (civil) 6350-6374 of 1997 [↑](#footnote-ref-32)
33. The Prisoners Identification Act, 1920, recently amended 1981 [↑](#footnote-ref-33)
34. th

    The Law Commission of India, 87 Report, 1920, http://lawcommissionofindia.nic.in/51100/report87.pdf [↑](#footnote-ref-34)
35. http://www.tn.gov.in/stationeryprinting/extraordinary/2010/305-Ex-IV-2.pdf [↑](#footnote-ref-35)
36. Adhikary, Jyotirmoy. DNA Technology in Administration of Justice. Lexis Nexis. 2007 pg. 259 [↑](#footnote-ref-36)
37. Justice, R.K. Abichandani, The Gene age, Legal Perspective, Conference at NLSAR University of law, Hyderabad held on 03/05/2003. [↑](#footnote-ref-37)
38. Binoy Viswam v. Union of India & Ors., Writ Petition (Civil) No. 277 of 2017 [↑](#footnote-ref-38)
39. Rohit Shekhar v. Narayan Dutt Tiwari & Anr, FAO(OS) No. 547/2011 [↑](#footnote-ref-39)
40. Govind v. State Of Madhya Pradesh & Anr on , 1975 AIR 1378, 1975 SCR (3) 946 [↑](#footnote-ref-40)
41. Lollia Paulina, also known as Lollia Paullina was a Roman Empress for six months in 38 as the third wife and consort of the Roman emperor Caligula. [↑](#footnote-ref-41)
42. Gautam Kundu v. Bengal, (1993) 3 SCC 418 [↑](#footnote-ref-42)
43. Sharda v. Dharmpal, (2003) 4 SCC 493 [↑](#footnote-ref-43)
44. The Role of DNA in Criminal Investigation– Admissibility in Indian Legal System and Future Perspectives , International Journal of Humanities and Social Science Invention ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714 www.ijhssi.org Volume 2 Issue 7 July 2013, PP.15-21. Retrieved on 31-8-2017. [↑](#footnote-ref-44)
45. Justice U.C. Shrivastava, Immunity from Self-Incrimination under Art. 20(3) of the Constitution of India.

    [↑](#footnote-ref-45)
46. Asit Kapoor v. Union of India, AIR 2004 Del 2003 [↑](#footnote-ref-46)
47. Khandu vs. State of West Bengal & Anr., AIR 1993 SC 2295 [↑](#footnote-ref-47)
48. Justice K.S. Puttaswamy(Retd) ... v. Union Of India And Ors, Writ Petition (Civil) NO 494 of 2012 [↑](#footnote-ref-48)
49. In People’s Union for Civil Liberties v Union of India (1997) 1 SCC 318 60 R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632. [↑](#footnote-ref-49)
50. Per H.L. Dattu, CJI, on 15th October 2015 Writ Petition (Civil) NO 494 OF 2012 between Justice K S Puttaswamy (Retd) and another v Union of India, [↑](#footnote-ref-50)
51. Orders dated 15.12.2017 in Writ Petition (Civil) NO 494 OF 2012 between Justice K S Puttaswamy (Retd) and another v Union of India [↑](#footnote-ref-51)
52. Aadhaar hearing: Data protection panel’s report coming in March, Centre tells SC Report to look at not only Aadhaar but all aspects of cyber security, says Attorney General K K Venugopal, The New Indian Express, New Delhi , 24-1-2018. [↑](#footnote-ref-52)