International Journal of Academic Research
ISSN: 2348-7666; Vol.5, Issue-1, January, 2018
Impact Factor: 6.023; Email: drtvramana@yahoo.co.in

Biometric evidence with a canon to right to privacy

Y. Bindu Madhavi
Research Scholar,
Dr. B.R. Ambedkar College of Law,
Andhra University, Visakhapatnam
and V Additional Junior Civil Judge, Guntur, A.P.

Abstract: It is evident that rights to privacy and fair information practices are part of the legal framework and come into play when dealing with any identification system like the biometrics mentioned here. Additional legal limitations may exist with these systems depending on the jurisdiction. Obtaining a biometric record of an individual, particularly from a secondary source such as his or her employer, in the course of an investigation, could be seen as "search." How the jurist

Key words: Biometric, Facial Recognition, temporarily divergent

Introduction

Every person has human right. Human right is not optional ".....throughout the web of English criminal law, one golden thread is always to be seen, that it is the duty of the prosecution to prove the prisoner's guilt"[1]

In the present day scenario, Biometrics plays a pivotal role in every walk of human life. Even it has gone to the extent of its usage, for fighting crime as well as identifying known and suspected persons are on the rise. Over the years, these biometric based systems have been in usage for verifying the claimed identity of individuals. Now the present question to be considered is whether biometrics usage has gone to the extent of disturbing and intruding up on the privacy of individual?, which Right to privacy is said to be the constitutional safeguard to the individuals. Let us see what the biometrics is?, what does right to privacy mean? and the judicial precedents in this regard.

What is Biometric? Biometrics refers to a science involving the analysis of biological observations, phenomena and characteristics. It commonly refers to technology that analyze human characteristics for security purpose.

The term *biometrics* is derived from the Greek words *bio* meaning *life* and *metric* meaning *to measure*. The two main types of biometric identifiers depend on either physiological characteristics or behavioral characteristics.

How Biometrics are Used

Biometric technologies are used almost exclusively for purposes of identification or authentication / verification. Identification is also often described as one-to-many matching. Automatic Fingerprint Identification Systems (AFIS) which match a single finger image against a database of images

1 Woolmington v DPP [1935] AC 462 is a famous House of Lords case in English law, where the presumption of innocence was first articulated in the Commonwealth

is one example. For the purposes of identification, a single biometric sample is compared to a collection of many other samples that can be linked to the sample owner's identity in the hopes that a match can be found. For policing organizations, both uses of biometrics may be required.

Different Types of Biometric Technologies:-

1 Body Odor

Each unique human smell is made up of chemicals knows as volatiles. These can be converted into a template by using sensors to capture body odor from non-intrusive parts of the body such as the back of the hand.

2 DNA

At present, use of DNA has largely been restricted to law enforcement activities involving one-to-one-matching. It is also, at present, relatively costly and time consuming to undertake. The additional information that can be gleaned from a DNA sample such as the presence of hereditary factors and medical disorders raises privacy concerns not associated with other biometric technologies. Current processes for obtaining DNA samples are also quite intrusive, requiring some form of tissue, blood or other bodily sample. Recently techniques have been developed that claim to be able to extract DNA from samples of hair or skin.

3 Ear Shape

Ear shape markings have already been used in the law enforcement field but have not as yet been used for other applications.

4 Facial Recognition

Facial Recognition technologies involve complex processes, usually requiring sophisticated artificial intelligence and machine-learning techniques. There are a number of technologies in this area that use either video or thermal imaging to capture the sample. capturing image, finding face in image, extract features, compare templates and declare matches. This system works by analyzing specific features of the individuals through a digital camera. These characteristics include information like the distance between eyes, the position of cheekbones, jaw line, chin, the width of the nose, etc. The data is gathered in the form of numerical quantities and then combined in a single code which is then used to uniquely identify each individual

5 Finger Scanning

Perhaps the most widely used biometric technology is finger scanning (which is also very similar to palm scanning.) Comparing with dots, spacing between two temporarily divergent ridges, spurs, bridges and crossovers. It has been reported that after comparing the database of fingerprints collected in more than 140 years, no two fingerprints were found to be the same, not even for the identical twins.

6 Hand Geometry

In hand geometry, a three-dimensional image of the hand is taken and measures of the shape and length of fingers and knuckles are made. Finger geometry is similar but uses only individual fingers. In industry terms, this was one of the first biometric technologies developed. Hand or finger

geometry is an automated measurement of many dimensions of hand and fingers

7 Iris Recognition.

Each person's iris has a unique and complexly patterned structure. The structure is a combination of specific characteristics called corona, crypts, filaments, freckles, pits, radial furrows and striations. It measures the iris pattern in the coloured part of the eye.

8 Keystroke .

Also known as 'keystroke dynamics, keystroke biometrics analyze typing rhythm. keystroke dynamic is an automated method of examining key stroke speed pressure, the time taken to type particular words and time elapsed between hitting certain keys.

9 Retinal Scan

The retina, the layer of blood vessels situated at the back of the eye, forms a unique pattern. Retinal biometrics are generally regarded as the most secure biometric method. A precise enrollment procedure is necessary, which involves lining up the eye to achieve an optimum reading. In this method, a beam of infrared light is cast into the person's eye when he looks through the scanner. As the retinal blood vessels readily absorb light, the amount of reflection varies. It is then digitized and stored in the database.

10 Personal Signature

This biometric technology is referred to as dynamic signature verification (DSV). It is the method of signing rather than the finished signature which is important and is not the same as the study of static signatures on paper (handwriting analysis.)It examines speed, direction and pressure of writing. The time that the stylus is in and out of contact with the paper.

11 Vein Pattern

Vein pattern recognition analyzes the distinctive pattern of veins in the back of the hand that form when a fist shape is made by the hand. The vein structure, or "vein tree," is captured using infrared light.

12 Voice Recognition

Voice recognition biometrics focus on the sound of the voice. This is quite distinct from the technology that recognizes words and acts on commands. It uses vocal characteristics by using a pass-phrase

The above are only illustrative but not conclusive. Due to recent evolving of scientific technology, there are number of types that have come into existence.

Now it is pertinent to refer what is Right to Privacy;

The Right to Privacy

In most of the common law constitutions, right to privacy is not given expressly to their citizens, but derived from judicial review and court decisions. The term "privacy" has been described as *"the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate with others. It means his right to withdraw or to participate as he sees fit. It also means the individual's right to control dissemination of information about himself; it is his own personal possession"*

Judicial activism has brought the Right to Privacy within the realm of Fundamental Rights. Article 141

of the Constitution states that "the law declared by the Hon'ble Supreme Court shall be binding on all courts within the territory of India." Therefore, the decisions of The Hon'ble Supreme Court of India become the Law of the Land. Apex court has come to the rescue of common citizen, time and again by construing "right to privacy" as a part of the Fundamental Right to "protection of life and personal liberty" under Article 21 of the Constitution, which states "no person shall be deprived of his life or personal liberty except according to procedures established by law". In the context of personal liberty, Hon'ble Supreme Court has observed "those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law."

Hon'ble Supreme Court on Right to Privacy

The Supreme Court has reiterated the Right to Privacy in the following cases:

1. [2]Kharak Singh v. State of UP this case pertains to domiciliary visits by the police during night. Apex Court held that the Regulation 236 is unconstitutional and violative of Article 21. It concluded that the Article 21 of the Constitution includes "right to privacy" as a part of the right to " protection of life and personal liberty". The Court equated 'personal liberty' with 'privacy', and observed, that "the concept of liberty in Article 21 was comprehensive enough to include privacy and that a person's house, where he lives with his family is his 'castle' and that nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy".

2. [3]Gobind v. State of M.P(1975) is another case on domiciliary visits. Hon'ble Supreme Court laid down that "...privacy-dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling State interest tests..."

3. [4]State v. Charulata Joshi, Hon'ble Apex Court held that "the constitutional right to freedom of speech and expression conferred by Article 19(1)(a) of the Constitution which includes the freedom of the press is not an absolute right. The press must first obtain the willingness of the person sought to be interviewed and no court can pass any order if the person to be interviewed expresses his unwillingness".

4. [5]R. Rajagopal v. State of Tamil Nadu, the Hon'ble Supreme Court held that the petitioners have a right to publish what they allege to be the life-story/autobiography of Auto Shankar insofar as it appears from the public records, even without his consent or Authorization. But if they go beyond that and publish his life story, they may be invading his right to privacy, then they will be liable for the consequences in accordance with law. Similarly, the State or its officials cannot prevent or restraint the said publication. It Stated that "A

2 AIR 1963 SC 1295

3 2 SCC 148

4 1999 (4)SCC 65

5 AIR 1995 SC 264

citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education among other matters. None can publish anything concerning 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……."

5. [6]People's Union for Civil Liberties (PUCL) v. Union of India, the Hon'ble Supreme Court held that the telephone tapping by Government under S. 5(2) of Telegraph Act, 1885 amounts infraction of Article 21 of the Constitution of India. Right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. The said right cannot be curtailed "except according to procedure established by law".

6. [7]In Mr. 'X' v. Hospital 'Z', for the first time Hon'ble Supreme Court articulated on sensitive data related to health. In this case, the appellant's blood test was conducted at the respondent's hospital and he was found to be HIV (+). His marriage, which was already settled, was called off after this revelation. Several persons including the members of his family and those belonging to their community came to know of his HIV (+) status and was ostracized by the community. He moved the Hon'ble Supreme Court by way of an appeal against decision of National Commission and argued that doctor-patient relationship, though basically commercial, is professionally, a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality." It however, held that although it was the basic principle of jurisprudence that 'every Right has a correlative Duty and every Duty has a correlative Right', the rule was not absolute and was 'subject to certain exceptions' in the sense that 'a person may have a Right, but there may not be correlative Duty, and the instant case fell within exceptions. The court observed that even the Code of Medical Ethics carved out an exception to the rule of confidentiality and permitted the disclosure in certain circumstances 'under which public interest would override the duty of confidentiality' particularly where there is 'an immediate or future health risk to others'. According to the court, the 'right to confidentiality, if any, vested in the appellant was not enforceable in the present situation, as the proposed marriage carried with it the health risk from being infected with the communicable disease from which the appellant suffered. The Hon'ble Supreme Court observed that as one of the basic human rights, the right of privacy was not treated as absolute and was 'subject to such action as may be lawfully taken for the prevention of crime or disorder or protection of health or morals or protection of rights and freedom of others."

7. [8]District Registrar and Collector v. Canara Bank, it was held, that "exclusion of illegitimate intrusions into privacy depends on the nature of the right being asserted and the way in which it is brought into play; it is at this point that the context becomes crucial, to

6 1997(1) SCC 301

7 1998(8) SCC 296

8 2005(1) SCC 496

inform substantive judgment. If these factors are relevant for defining the right to privacy, they are quite relevant whenever there is invasion of that right by way of searches and seizures at the instance of the State."

If one follows the judgments given by the Hon'ble Supreme Court, three themes emerges:

1. that the individual's right to privacy exists and any unlawful invasion of privacy would make the 'offender' liable for the consequences in accordance with law;

2. that there is constitutional recognition given to the right of privacy which protects personal privacy against unlawful governmental invasion;

3. that the person's "right to be let alone" is not an absolute right and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others;

8. [9]***Maneka Gandhi v. Union of India,*** wherein this right is recognized, subject to legal restrictions satisfying the requirements as laid down in the Maneka Gandhi case. However, if the courts were to address the issue of right to privacy under Article 21 afresh, there is little doubt that it would conclude that there does exist a right to privacy. On a harmonious interpretation of the legal principles as laid down by the Supreme Court at different points of time, it is sufficient to conclude the existence of right to privacy under Part III of the Constitution. Privacy is also a feature of the dignity of an individual that the preamble to the Constitution assures every individual. Thus the right is not merely a negative mandate upon the state not to encroach upon the private space of the individual but is also a positive affirmation on the state to create adequate institutions that would enable one to effectively protect his private life.

9. Hon'ble Bombay High Court, passed orders requiring UIDAI to provide biometric information to CBI for investigation purposes with respect to a criminal trial. The said order was challenged by filing [10]**Special Leave Petition (Criminal) No. 2524 of 2014,** in which orders dated March 24, 2014 were passed by the Hon'ble Apex Court restraining the UIDAI from transferring any biometric information to any agency without the written consent of the concerned individual. The said order is in the following terms:

> "In the meanwhile, the present petitioner is restrained from transferring any biometric information of any person who has been allotted the Aadhaar number to any other agency without his consent in writing.

More so, no person shall be deprived of any service for want of Aadhaar number in case he/she is otherwise eligible/entitled. All the authorities are directed to modify their forms/circulars/likes so as to not compulsorily require the Aadhaar number in order to meet the requirement of the interim order passed by this Court forthwith."

9 AIR 1978 SC 597, 621

10 *Unique Identification Auth. of India and anr.* v. *Central Bureau of Investigation*

10. The Hon'ble Apex court considering the union government making adhaar as mandatory in WRIT PETITION (CIVIL) NO 494 OF 2012,[11]JUSTICE K S PUTTASWAMY (RETD.),AND ANR...VERSUS UNION OF INDIA AND ORS...Respondents Judgment Dated 24-08-2017 considered all the above said decisions and reference was answered as below

Our Conclusions

1 The judgment in M P Sharma holds essentially that in the absence of a provision similar to the Fourth Amendment to the US Constitution, the right to privacy cannot be read into the provisions of Article 20 (3) of the Indian Constitution. The judgment does not specifically adjudicate on whether a right to privacy would arise from any of the other provisions of the rights guaranteed by Part III including Article 21 and Article 19. The observation that privacy is not a right guaranteed by the Indian Constitution is not reflective of the correct position. M P Sharma is overruled to the extent to which it indicates to the contrary.

2 Kharak Singh has correctly held that the content of the expression 'life' under Article 21 means not merely the right to a person's "animal existence" and that the expression 'personal liberty' is a guarantee against invasion into the sanctity of a person's home or an intrusion into personal security. Kharak Singh also correctly laid down that the dignity of the individual must lend content to the meaning of 'personal liberty'. The first part of the decision in Kharak Singh which invalidated domiciliary visits at night on the ground that they violated ordered liberty is an implicit recognition of the right to privacy. The second part of the decision, however, which holds that the right to privacy is not a guaranteed right under our Constitution, is not reflective of the correct position. Similarly, Kharak Singh's reliance upon the decision of the majority in Gopalan is not reflective of the correct position in view of the decisions in Cooper and in Maneka. Kharak Singh to the extent that it holds that the right to privacy is not protected under the Indian Constitution is overruled.

3 (A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian Constitution;

(B) Life and personal liberty are not creations of the Constitution. These rights are recognised by the Constitution as inhering in each individual as an intrinsic and inseparable part of the human element which dwells within;

(C) Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III;

(D) Judicial recognition of the existence of a constitutional right of privacy is not an exercise in the nature of amending the Constitution nor is the Court embarking on a constitutional function of that nature which is entrusted to Parliament;

11 indiankanoon.org/doc/91938676/

(E) Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level privacy sub-serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interests which lie at the foundation of ordered liberty;

(F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being;

(G) This Court has not embarked upon an exhaustive enumeration or a catalogue of entitlements or interests comprised in the right to privacy. The Constitution must evolve with the felt necessities of time to meet the challenges thrown up in a democratic order governed by the rule of law. The meaning of the Constitution cannot be frozen on the perspectives present when it was adopted. Technological change has given rise to concerns which were not present seven decades ago and the rapid growth of technology may render obsolescent many notions of the present. Hence the interpretation of the Constitution must be resilient and flexible to allow future generations to adapt its content bearing in mind its basic or essential features;

(H) Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them; and

(I) Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual.4 Decisions rendered by this Court subsequent to Kharak Singh, upholding the right to privacy would be read subject to the above principles. 5 Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put

into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union government while designing a carefully structured regime for the protection of the data. Since the Union government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B N Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in this judgment.

11. The Hon'ble apex Court in the case of [12]PUCL v. Union of India has approved the recommendations of the High Powered Committee headed by Justice D.P. Wadhwa, which recommended linking of Aadhaar with PDS and encouraged State Governments to adopt the same.

The Hon'ble Apex Court in [13]State of Kerala & others vs. President, Parents Teachers Association, SNVUP and Others has directed use of Aadhaar for checking bogus admissions in schools with the following observations:

Thus, it is evident that rights to privacy and fair information practices are part of the legal framework and come into play when dealing with any identification system like the biometrics mentioned here. Additional legal limitations may exist with these systems depending on the jurisdiction. Obtaining a biometric record of an individual, particularly from a secondary source such as his or her employer, in the course of an investigation, could be seen as "search." How the jurisdiction's laws limit the process of "search" and whether there is an expectation of privacy within those laws could very well affect the legitimacy of obtaining a biometric record. Obtaining a biometric involuntarily, even if directly obtained from an individual, may be viewed as forced self-incrimination.

For the last two decades science has developed biometric based forensic evidence. New technologies to prove the identification were discovered. DNA, facial recognition technologies, retina identification and other biometric identification technologies were discovered. They are being used as evidence to prove the identification of accused. After terrorist attacks over the world trade center, the demand for using these technologies was increased. The increase in terrorism in various countries also demand the use of the technologies. Countries are maintaining biometric data. In our country too biometric data was collected at the time of issuing AADHAR cards. Recently in Gova, CBI has filed an application U/Sec.91 Cr.P.C to receive biometric data available with the unique identification authority of India (the authority was established to collect and maintain biometric data which was collected to issue AADHAR cards) to prove the identification of an

12 indiankanoon.org/doc/1168094/

13 indiankanoon.org/doc/31308426/

accused in a rape case, which was discussed supra. Recently a San Francisco judge ruled that biometric facial recognition could be submitted as legal evidence in a trial. It's the first time such evidence was used in a criminal trial, and opens the door to a series of legal questions, namely because facial recognition technology is neither definitively accurate nor up to basic legal standards for evidence.

Biometrics – the risks

It is essential to understand the risks of biometrics in order to develop relevant policy and legislative frameworks on their development and use, and minimise the potential negative impact they may have. The very nature of biometrics can lead several problems: the data processed is at risk of being misused and is subject to fraud; it can result in misidentification and inaccuracies; its nature renders it exclusionary and its unregulated retention raises questions function creep and the safety of the data itself.

In addition, whilst recognizing that biometrics is in and of itself is not harmful, the policy and legal void in which it is used fails to regulate and limit its purpose. Thus, it can potentially be seen and used as a tool for surveillance through profiling, data mining and big data. Protecting privacy in biometric systems: the challenges.

The Problem of Mismatching The typical errors associated with the use of biometrics are 'false positive' matches and 'false negative' matches. Correct matches will result in either a true positive match (the "new" biometric sample matches with an "old" sample collected earlier from the same individual), or a true negative match (the "new" biometric sample is found to correctly have no match with a single sample collected earlier in the case of authentication/verification, or with any of the "old" samples in the case of identification).

Whenever a balance between individual needs and societal needs must be struck, the development of legislation is perhaps the best way to achieve this balance. Although most Western jurisdictions have legislated privacy and information handling practices, there are some notable exceptions, with considerable variation in the laws. This means that separate legislation to cover the use of biometrics is called for. Public concerns about multi-purpose identification processes have been well documented and the unrestrained use of biometric technologies by disparate groups – police, employers, social benefit administrators, etc., would undoubtedly meet with the same concerns. The use of biometrics needs to conform to the standards and expectations of a privacy-minded society.

Biometric vulnerabilities

An early attack on fingerprint biometric authentication is called the gummy bear hack, and it dates back to 2002 when Japanese researchers, using a gelatin-based confection, showed that an attacker can lift a latent fingerprint from a glossy surface; the capacitance of gelatin is similar to that of a human finger, so fingerprint scanners designed to detect capacitance would be fooled by the gelatin transfer.

[14]In 2015, Jan Krissler, also known as "Starbug," a Chaos Computer Club biometrics researcher,

14 Internet source

demonstrated a method for extracting enough data from a high-resolution photograph to defeat iris scanning authentication;[15] in 2017, Krissler reported defeating the iris scanner authentication scheme used by the Samsung Galaxy S8 smartphone. Krissler had previously recreated a user's thumb print from a high-resolution image to demonstrate that Apple's Touch ID fingerprinting authentication scheme was also vulnerable.

Conclusion

Although policing is primarily a law enforcement activity, those in the policing profession must have at least a working knowledge of a wide variety of other types of activities in order to become good at law enforcement. Modern policing requires its practitioners to see beyond their realm in order to be truly effective. The law enforcement area is probably the largest biometric user group. Primarily AFIS and palm-based technologies are used as an extension of traditional human processes. However, there have been applications based on other biometric technologies that are entering this area. As one example, United Kingdom authorities have tested the use of facial recognition to match images captured by surveillance cameras with a database of "criminals."

Thus from the above enunciation of judicial activism, it is limpid that in today's digital world, the fundamental right to privacy safeguards who we are and supports our on-going struggle to maintain our autonomy and self-determination in the face of increasing state power. Technological advancements are providing unprecedented opportunities to empower people, but also pose the potential for significant negative impacts on basic human rights. These consequences are a particular risk in the deployment of biometrics, which remains unregulated by laws relating to the protection of personal data and privacy as well as the biometric industry, which fails to incorporate privacy and data protection standards in their own procedures. Emerging challenges include the ethical impact of identification programmes, the need to consider cultural and social norms, and the dangers of the assessment of data.

Since the Law is a living process, which changes according to the changes in society, science, ethics and so on. The Legal System should imbibe developments and advances that take place in science as long as they do not violate fundamental legal principles and are for the benefit of public at large and for the society. The criminal justice system should be based on just and equitable principles. Legislation, policies and procedures must be developed and conveyed to biometric users. When a biometric is to be collected, how it is used, to whom it is disclosed and how long it is retained must be clearly understood. Further there is a great deal of debate these days about the impact of the newest identification technology, DNA typing, facial recognition and other biometric evidence on the criminal justice system. The introduction and rapid diffusion of this powerful technique over the past two decades or so has raised a host of important question including:

How accurate, discriminating, and reliable?

How do biometric evidence measure these attributes?

15 Websource

How do we police the application of DNA typing?

Facial recognition and other biometric evidence to minimize errors?

How inclusive should DNA, facial recognition and other biometric evidence databases be?

What kind of threat do they pose to individual privacy and to civil liberties?

What is the relationship between the criminal justice application of DNA typing facial recognition and other biometric evidence and other applications in areas like health care, immigration control, and scientific research?

Hence in the present digital world, the usage of biometrics has predominant role, in which the criminal investigation is not an exception. However it should be the endevour of every one to uphold the dignity and protect the right to privacy of an individual. Nevertheless, there are numerous queries with regard to the use of biometrics as evidence. Still it is in infant stage and needs lot of discussions and deliberations on this aspect. Further there must be uniform enactment/Act which shall incorporate mode of its use, manner, rules governing, regulations of, etc for using biometric based evidence.