CHAPTER THREE

Role of Scientific Aid in the Investigation of Crime
“.... If matters arise in our law which concern other sciences or faculties, we commonly apply for the aid of that science or faculty which it concerns. This is an honorable and commendable thing in our law. We approve of them and encourage them as things worthy of commendation.”

- Justice Sauders

Crime is as old as human civilization and so are its relative concepts of punishment and conviction. As the society developed, laws were enacted for controlling the crime, for sentencing of the conviction and for implementing the punishment. Criminal cases were put on trial in the court of law to determine the guilt or innocence of the accused. The accused, if proved guilty, was convicted and punished by the court. In criminal investigation, the traditional methods deployed by the investigating agencies could not meet the demand of the society for a crime free existence. The application of the modern technology and scientific aid in the investigation was thus understood to be a necessity for drastic increase in the conviction rate of various crimes and, more importantly, for lowering the rate of wrongful conviction. It was blatantly clear that the conviction rate for certain offences in the country was not in proportion with the rate of that crime. The reason for such a mismatch of conviction rate and crime rate is due to improper (and in some cases unbalanced) utilization of scientific aid and forensic science in criminal investigation. Moreover flexibility is the greatest virtue of law and thus its applicability should also be flexible rather than being a rigid insistence of strict format. Moreover, law is dynamic in nature. It is anything but static. As society,
science, technology, ethics and other thing changes, the law should also change accordingly. The legal system should keep on absorbing developments and advances that take place in science, as long as these changes benefit the society and do not violate the fundamental legal principles. Freedoms of the individual are not meant to be subjected to improper means howsoever justified the ends may be. Therefore there is a need to replace the ‘third degree methods’ by better refined and sophisticated techniques. In this pursuit, scientific aid more importantly Narco-analysis, Brain Mapping, Polygraph Test, DNA Fingerprinting and Computer Forensics could play a instrumental role. For example, Narco-analysis test can evolve as a viable and effective alternative to the existing inhumane third degree methods.

**The application of Scientific and Technical Tools in Criminal investigation - Two celebrated case studies**

The history of the role of scientific testimony and its admissibility as evidence involved two very landmark and interesting cases that illustrated the difficulties that courts confronts while determining the standard for admissibility of novel scientific evidence in a criminal trial.

**The Frye case**

Prior to 1923 in the United States, most courts treated rules governing the admissibility of scientific evidence as derived from Common law and there was no codification of specific rules. In 1923, however the landscape changed for the role of
novel scientific evidences in criminal investigation owing to a murder case in Washington, D.C. James Frye was on the trial for murder. As part of his argument, he sought to introduce the result of a test that utilized a machine that could be considered the forerunner of today’s polygraph. He pleaded innocent on the basis of the result of the test from that machine. The prosecution objected to the admission of his novel evidence and the judge ruled in the favour of the prosecution. On appeal, the appellate court upheld the trial judge’s order stating that for novel scientific technique to be admitted as evidence, not only it must meet the relevancy standards but also one additional hurdle of ‘general acceptance’\(^{71}\). The court opined in this respect that it is very difficult to draw a line between experimental and demonstrable stages of any scientific principle or discovery. Finding force with the argument that evidentiary force of scientific principle must be found within the twilight zone of acceptability, the court will go a long way in admitting expert testimony deduced from a well recognized scientific principle or discovery only when the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field to which it belongs\(^{72}\).

Though the matter was settled for now, the court did not elaborate on as to what constituted ‘general acceptance’. In fact, this issue has never been clearly decided by the court. However by default, it began to mean that for general acceptance, the technique and principle should have been published in a peer reviewed journal or other equivalent exposure to the field. This gave birth to an anomaly in the scientific world where there are numerous scientific principle endeavors which have never been published but there are numerous examples of


\(^{72}\) Frye v. United States, 293F, 1013, 1014(D.C.Cir. 1923)
techniques that have been published and later shown to be unreliable. Whatsoever, this legal principle remained the yardstick for evaluating the admissibility of scientific techniques for the federal courts and about half of the States for nearly 50 years. During that time a number of novel scientific techniques were subject to “Frye challenge” in various courts which included Voiceprint spectrography, Blood Spatter Pattern Analysis, Polygraph analysis, and even DNA Typing techniques.

In the year 1975, the Congress, for the first time, approved an evidence code. This had been proposed by the U.S. Supreme Court as a preliminary draft in 1969. The initial set of rules of evidence contained a specific rule 702 which stated that the proponent of expert testimony had the burden of demonstrating that the expert was qualified and that the opinion evidence would be deemed helpful to the fact finder i.e. the judge. After the new evidence code was adopted by Congress, federal and many state courts became divided as to whether Frye or the new Federal code should be used to determine the admissibility of the scientific evidence. The question was addressed and settled by the U.S. Supreme Court in *Dubert v. Merrill-Dow*, which then became the landmark with respect to admissibility of scientific evidence in the court of law.

**Dubert v. Merrill-Dow**

The facts of the case was that the plaintiff in Dubert v. Merrill-Dow, in federal District court, was a pregnant woman, who took Bendectin, a Merrill-Dow product that had been prescribed for many years to relieve Nausea that occurred during pregnancy. When the baby to plaintiff was born with birth defects, she sued Merrill-Dow, claiming that Bendectin caused the birth defect. Since biochemical causes of
birth defects were not fully understood, there was no direct way for Dubert to establish that Bendectin was the cause of the defects. Instead, the plaintiff had to resort to statistics in regard to the study of the cause and effects of disease on large populations. The plaintiff and defendant both fielded statisticians as experts to determine whether the instance of birth defects among women who took Bendectin during pregnancy were statistically greater than birth defects in the general population or not. The plaintiff’s expert concluded that there was a significant increase in birth defects among Bendectin user’s babies, whereas the defendant’s expert concluded that the plaintiff’s expert did not use methods that were generally accepted by the scientific community in reaching their conclusions. The district federal judge, after relying on Frye judgement ruled in the favor of Merrill-Dow. Dubert appealed and eventually the case reached the U.S. Supreme court. The US Supreme court ruled that the trial judge had used the wrong standard of admissibility in reaching to his conclusion. The Supreme Court set the law that the federal courts could not use the Frye rule any more in deciding question about the admissibility of scientific or technical evidence, and that the doctrine of general acceptance was not the proper yardstick. Instead, the courts must use the “Federal Rules of Evidence” as relevant standard while evaluating the admissibility of novel scientific or technical evidence. The Court drew particular attention to FRE 702, reproduced here:

“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.”
Further in interpreting the Federal Rules including 401, 402, 403, and 702, the court indicated that the judge must be the gatekeeper who decides when novel scientific evidence is admissible. In doing so, the court went as far as to suggest several criteria that a judge could use in the gatekeeper role. These criteria were not meant to be exhaustive, but only suggestive:

(a) **Falsifiability**: If the underlying theory or principle behind a novel technique has been repeatedly tested to see if it is false and in all cases the theory is verified, then it can be a good measure of validity. This is not amenable to all the principles and proper research design must be implemented for this to be a valid criterion.

(b) **Knowledge of error rates**: If the error rates of the result of a technique are known or can be estimated, then a judge could presumably make some determination about the reliability and validity of a technique.

(c) **Peer review**: Certainly a technique or method or principle that has survived the peer review process and has been found worthy of publication demonstrates some level of scientific validity. This is dependent, however, on the quality and scholarliness of the journal in the applicable field.

(d) **General acceptance**: The Supreme Court of U.S. never intends to discard general acceptance as an acceptable criterion for determining scientific validity. The court concluded that this should not be the only criterion and that there exist other, perhaps better ones. The court did not, however, seek to define what it meant by general acceptance.

---

In addition, the court’s decision mandate that novel scientific techniques must be based on scientific principle, not speculation, and that the scientific basis for the principles had to be a demonstrated.

Some of the modern techniques in aid to scientific criminal investigation and prosecution are described in brief.

**Polygraph or Lie detector Test**

Polygraph test or psycho-physiological detection is one of the important scientific tools for investigation. More popularly known as lie detector test, it is a technique which measures and records the physiological parameters of the human body such as blood-pressure, pulse rate, respiration and skin conductivity while the subject responds to question relating to the crime, crime scene or the victim. Since the Polygraph test measures the changes caused by Autonomous Nervous System, which are beyond reasonable control of an individual, it transpires into change of response when the subject tries to tell a lie.

The polygraph on the other hand is an instrument that records certain physiological changes in a person’s body going through the interrogation in order to get hold of deception and lies for investigation\(^7\). No definition of a polygraph has been found in any Indian legislation. However it is defined in United States Employee Polygraph Protection Act of 1988 as,

“Polygraph means an instrument that:

(A) Records continuously visually, permanently and simultaneously as minimum instrumentation standards; and

(B) Is used, or the results of which are used for the purpose of rendering diagnostic opinion regarding the honesty or dishonesty of an individual”.

The Polygraph machine was further refined by Keeler by adding a Psychogalvanometer to record the electrical resistance of the skin. Wigmore (a legal author and an expert in the common law) in 1970 supported the legal use of the Polygraph test in Criminal investigations. He noted three probative use of Polygraph with respect to criminal investigation, namely:

a) The Investigation/Police authorities may use it as a clue to obtain external data which can be used as an evidence;
b) The disclosure of lies may force the subject not to concoct the facts; and
c) The recorded curves may disclose the general emotional consciousness of guilt and that can in turn guide the Police/Investigative authorities in their hypothesis.

The United States Supreme Court has held that a Miranda warning is sufficient to allow admissibility of a confession before a Polygraph examination. The evidence of Polygraph is admitted in most of United States Court under stipulation that trail of a fact has to weigh up the probative value of the matter against the prejudicial effect inflicted upon the defendant. Professor David Lykken, a PhD from the University of Minnesota, has written that:

76 Explanation of rights that must be given before any custodial interrogation, stemming largely from the Fifth Amendment privilege against self-incrimination.
77 A person, or group of persons who determine facts in a legal proceeding, usually a trial.
"Judicious use of the Polygraph in the Criminal investigation not only can improve the efficiency of police work but could also serve as a bulwark to protect the innocent from false prosecution. In fact, I believe that if the police can use the Polygraph wisely, it can greatly facilitate their work."

In Australian context also, there is no legal impediment for the use of Polygraph test as a tool for investigation other than the Lie Detector Act NSW 1983 which in certain circumstances prohibits the use of Polygraph on the subject or the accused.

The underlying principle behind Polygraph technique is to make the subject or the accused in case of criminal investigation nervous and shaky resulting into creation of emotion of fear and consequently leading to physiological changes which in turn are captured by the Polygraph instrument. Thus when a person is lying, the fear of getting caught or entrapped causes mental excitation and in an attempt to conceal the excitation, adrenal glands are stimulated to secrete adrenalin which on entering the blood stream steps up the blood pressure and rate of pulse and respiration of the individual. All these recordings are collectively known as polygraph, which is evaluated by a professional to ascertain the credibility of any witness or accused. The question asked may be such to which answers may be known to the subject (For e.g. the name and address of any particular person or his own self) or related to the crime or criminal or the victim. More broadly, the questions asked to the subject can be categorized into\textsuperscript{78}:

i. \textit{Control questions:} These are the questions which are most commonly asked during the Polygraph examination. These questions are irrelevant to the facts of the case

\textsuperscript{78}Murray Kleiner, “Handbook of Polygraph testing”, Academic Press, New York, 2002
Role of Scientific Aid to Investigation in Administration of Criminal Justice in India- A Critical Evaluation

being investigated but they are intended to provoke distinct psychological responses, as well as false denials. They do not directly relate to the crime under investigation, but to a similar situation in which the answers may have a feeling of concern with respect to either its truthfulness or its accuracy.

ii. **Direct Lie Questions:** When the subject is telling the truth, these questions are framed so as to make the subject deliberately lie. The psychological responses are subsequently compared to detect lying.

iii. **Guilty Knowledge Questions:** These are multi-choice type questions relating to crime under investigation where one choice would contain information relating only to the crime investigation (and sometimes not) which the real culprit could only know.

iv. **Peak of tension Questions:** Peak of tension questions are framed when some of the important details of the offence in question are not made known to the subject. These questions are framed in such a way that only one question will have bearing upon the matter under investigation and all others come close to the guilty knowledge.

In India, since 1974 more than 3000 polygraph tests have been conducted. Indian Courts had never objected to polygraph test or for any scientific aid and many High Courts have passed orders in favor of scientific tools. It was held by the court in *Ramchandra Reddy and Ors. v. State of Maharashtra*:

“In this test the polygraph is taken which gives this reaction and an expert would then explain these reactions in the court which would be his reading of the polygraph from which would flow his conclusion which are to be admitted or not

---

79 Criminal Writ Petition No.1924 of 2003(SC)
admitted by a Judge on appreciation of the statement and the objections raised theret”

But recently in May 2010 the Supreme Court in case of Smt. Selvi & Ors. V. State of Karnataka\(^8\) had objected to these scientific investigation tools without the prior consent of the subject/accused.

**Polygraph-Modus Operandi**

Modern Polygraph recording has become computerized. The apparatus consists of a computer, a combination unit that provides for magnification of the physiological signals and their conversion to the digital form, and a printer. The Polygraph test consists of a series of psychological tests where changes in physiological parameters or attributes are recorded on three aspects of human physiology, viz\(^8\) –

i. Pneumograph tracing,

ii. Electrodumal activity tracing, and

iii. Cardiovascular tracing

The first relates to respiration, the second to skin conductance or skin resistance and the third with blood volume and pulse rate. If a person tries to conceal or tell a lie, physiological changes like increase or decrease in blood volume, increase or decrease in heart rate and changes in respiration, perspiration takes place. If the

\(^8\) AIR 2010 SC 1974

person is truthful, the organs exhibiting such physiological changes function in normal pattern.

**Polygraph Test Stages**

Generally polygraph test is conducted in three stages:

(i) *The Pre-test interview:* It includes a brief introduction by the examiner to the subject followed by a presentation of the procedure and legal aspects of the test. The consent of the subject is then taken making him aware of his legal rights. Enquiries regarding subject’s medical conditions are made before the Pneumograph, the Sphygmomanometers and Electrode are placed on the subject.

(ii) *The Chart Collection or Examination Proper:* This includes the actual test where questions prepared in advance are put to the subject who has to reply in either affirmative or in negation. Some of questions are irrelevant and some are relevant. The instrument records changes by means of a needle on the graph paper.

(iii) *The Post-test Interview:* In this stage the result of the test is discussed with the subject in order to analyze about deception of attempted/unresponsive questions.

The Polygraph so obtained does not directly detect whether the person is speaking truth or not but the examiner carefully analyzes the pattern of arousal responses and on that basis credibility of the individual is inferred. This inference or
assessment is called ‘Diagnosis’ of truthfulness or deception. All these collected reactions are put together in corroboration with the other gathered evidence.

Validity & Reliability

As to the accuracy of the Polygraph testing in the last decade alone, some 250 studies have been done. Also since 1980, 10 separate studies based on 1909 real cases had shown that there was around 97% accuracy rate for truthful subjects and 98% for deceptive ones. The skeptics have always raised concern regarding the unachievable 100% accuracy of Polygraph technology; however the same skeptics fail to consider that there is not a single scientific test that is 100% perfect in the entire world including the Psychological and Psychiatry assessment involving clinical diagnosis.

Psychological disorders are subjective in nature and sometimes are wrongly classified and challenged by the other experts. In DNA testing too, cross contamination can occur in several cases or many a times fingerprints can be wrongly matched or handwriting has been misinterpreted by the experts and even eye witnesses can make blunders in identifying an offender. Further, admissibility of evidence does not mean that it is valid. It is worth noting that no matter how invalid eyewitness and psychiatric findings could be, they often are accepted and recognized, legally and judiciously as admissible evidence.
Current Usage within Criminal & Private Investigations

Polygraph usage has proven its utility within the following realms during criminal investigation:

i. Short listing suspects.

ii. Identifying false complaints.

iii. Evaluating informants to determine the authenticity of information provided.

iv. Providing a new "way" to an investigation when all other doors to investigation have been exhausted.

v. Helps in focusing on main part of enquiry.

vi. Collecting additional information and evidence that may be required during investigation or trial.

vii. Helps to focus the investigation on particular suspects or witness.

Other uses within the private realm include:

i. In cases of Professional misconduct allegations e.g. Doctors, Accountants etc.

ii. In cases of Theft/Fraud investigations inside the company.

iii. Civil investigations.

iv. Checking the veracity of affidavits/statements given by employees.

v. Help in investigating malicious and false allegations against co-employees.

vi. Unfair removal.

vii. Drug abuse by athletes or employees.

viii. Determining Disputes of fact.

ix. Investigating Sexual harassment claims/allegations by the complainant.
Critical Analysis of Polygraph Test

Polygraph is merely a machine that reads the physiological response of the body of an individual and cannot miraculously "know" when a subject is lying. Poor response by the test can occur because of many reasons. Firstly, different people respond differently to varying stresses. Many subjects react in extreme ways to both positive and negative stimulation while some others have no physical response whatsoever. Some subjects can even trick the Polygraph test subject to operator’s error who is involved in conducting the test. There is no way to ascertain the veracity of the statements made during the Polygraph test without any hard evidence already existing to match the facts. Hence the test sometimes turns out to be a futile exercise. If a subject is delusional or have some mental disorder and he truly believes that whatever he is saying is truth then he can easily pass the Polygraph test.

Secondly, the subject can exhibit anxiety due to other reasons except lying and thus it can result into unreliable outcomes. Other human attributes like nervousness, sadness, embarrassment, anger and fear could also lead to alteration in one's heart rate, blood pressure or respiration rate. Several medical conditions such as cold, constipation, headache or neurological and muscular problems can also alter physiological state which could wrongly be read by the Polygraph machine as an elevated response. Thus, in this test the device measures the anxiety but the test cannot determine the reason for such an anxiety. The subject can be a good liar or a psychopath. Or in other words, a non elevated response to question should not be construed as proof of innocence.
Thirdly, the results of the test are not perfect due to the subjectivity of the examiner who is conducting the test. The examiner due to their personal bias or otherwise may favour or be against the accused and could manipulate the result leading to either his innocence or conviction. Lastly, there is no conclusive evidence that the Polygraph test can detect lies. The machine at best can only measure the changes occurring in the blood pressure, pulse rate and respiration rate of the person undergoing the test. Till date no scientific formula or law has been developed which can ensure a direct relation between these physiological changes occurring in the body of the subject and guilt or fear of lying in the mind of the subject.

Even after several experiments and researches, Scientists and Researchers have not found any scientific evidence that Polygraph test can detect the subject’s deceptions better than non-experts using traditional investigational method of interrogation on the same subject. There are no machines and no experts which can detect who among the given group of random person are lying or telling the truth.

Despite several known drawbacks in the Polygraph test, one of the main reasons why it is still used is the belief that many of the subjects will frighten away due to fear of being caught or the liars and cheats who are trying to fake any commission of the crime will abstain from approaching authorities or it will force the accused of a crime to spit out the confession of their wrong doing. Therefore the administrator of the machine wants people to believe that the machine can catch them if they lie, although he himself very clearly knows that the machine can’t do everything.
Another main reason for the use of the Polygraph test is the pragmatic fallacy factor. It is pertinent to point out that till date, no scientific study has been published offering convincing evidence regarding the validity of the Polygraph test. Even if it is believed that the Polygraph test can detect intentional lies, one cannot differentiate between honestly mistaken answers and celebrated lies. However in India the law is very clear, “It is better that ten guilty persons escape than that one innocent suffer”. Hence, the use of Polygraph test should be confined to proofing the innocence of the subject rather than his guilt.

**Narco-Analysis Test**

Narco-Analysis or Narcosynthesis is another important technique for crime detection during interrogation across the world. It is a kind of psychotherapy which is conducted on a person by suppressing his/her self consciousness and inducing him into semi-sleep condition with the help of scientific drugs. It is assumed that since the person has reached to a tranche state, known as ‘Twilight state’ where it is difficult to lie for him, any attempt to extract information about any particular criminal activity could yield fruitful results. Thus it is believed that a person’s way of thinking can be restrained without affecting his/her memory.

The term Narco-analysis is derived from a Greek word “narke” which means anesthesia and is used to describe a technique of diagnosing and giving the psychotherapy with the help of psychotropic drugs. It is also known as drug hypnosis
or a truth serum or a combination of hypnosis or narcosis\textsuperscript{82}. It was J. Stephen Horsely who first coined the term Narco-analysis in 1936. Thus it is method to make human thought and communication manageable. The drug used for this purpose is called ‘Truth serum’.

Generally the Truth serum is an anesthetic and sedative drug. A few of the best known one include:

i. Scopolamine
ii. Sodium Pentothal
iii. Midazolam
iv. Sodium Amytal
v. Pentobarbital
vi. Sodium Thiopental

\textit{Narco Analysis - Modus Operandi}

Following are the important things involved in the tests:

(i) Video recorder
(ii) Tape recorder
(iii) Disposable syringe
(iv) Distilled water
(v) Prescribed truth drug

\textsuperscript{82} Caesar Roy, “Narco Analysis Test-Infringement of Individual Fundamental Rights and Its Value as Evidence”, \textit{Criminal Law Journal}, March 2009, p 69
Every minute detail of the test is video graphed while it is being conducted. Along with the video, the whole procedure is also recorded on an audio tape.

Disposable syringe and distilled water is used for the purpose of conducting the test. The drug which is to be used while conducting test is to be mixed with some distilled water. The dosage of Truth Serum depends upon the suspect’s sex, age, health and physical and mental condition. Generally, 3 gram of Truth drugs of barbiturate class like sodium pentothal, sodium amytal etc. is required for the test which is dissolved in 3000ml of distilled water. The resultant solution is administered intravenously along with 10% of dextrose at an interval of 3 hours to the suspect/accused. At the time of the test the presence of the following is necessary:

(i) Physician
(ii) Neurologist
(iii) Cardiologist
(iv) Anesthetist
(v) Lawyer

Precautions and Guidelines

The following precautions should be taken for fruitful result of test:

(i) The test should be conducted in a well-lit room which is otherwise quiet.
(ii) Prior consent of the subject has to be obtained and the person subjected to the test should be given an option if he or she wishes to avail the test.
(iii) Consent should be recorded and it should be done before a judicial magistrate.
(iv) The physical and emotional implication along with the legal implications of the test should be explained to the subject by the lawyer having access to him or her or by the police so that he or she submits himself or herself to the test voluntarily.

(v) The person subjected to the test should be clarified that his or her statements so made shall not be a “confessional statement” to the magistrate but a statement to the police.

(vi) The entire process should be videotaped.

(vii) The drug should be diluted at 8.66% and should be injected showing at intervals throughout the interview.

(viii) The drug should be administered such that a state between sleep and wakefulness is maintained.

(ix) Caffeine should be used to prevent the subject from going into deep sleep.

(x) The interview should not exceed one hour of time;

(xi) The actual recording of test shall be done in the presence of a lawyer.

(xii) Manner of information received must be completely narrated in full and must be recorded;

(xiii) In India the test should be conducted as per norms of the NHRC of India.

(xiv) Narco analysis cannot be conducted without the consent of the subject and order of the court.

**Guidelines for Interrogating the Suspect during Narco Analysis Test**

i. The suspect is not given food 5-6 hours before the start of the test and alcohol containing food and medicine should also be avoided.
ii. The suspect must always be attended by the physician/psychiatrist from the
time of injection until the initial narcosis worn off.

iii. Careful observation is necessary if properly administered drug dosages
cause no alarming physiological effect on pulse rate as well as respiratory
rate.

iv. Larger dosages are too dangerous as it may lead to Sedative stage,
unconsciousness with exaggerated reflex (hyperactive stage), unconsciousness
without reflex even to painful stimuli, and even death. Therefore, Narco
analysis test should be performed with great care and caution and in the
supervision of experts.

v. If the suspect goes to deep sleep then by the use of anti-narcotics stimulants
the suspect should be awake in a minute.

vi. Emergency resuscitation equipments should remain available because in
certain cases incident of laryngospasm do occur.

vii. The quantity of drug depends upon the suspect’s sex, age, health and physical
and mental condition.

viii. The interviewee should be aware of the purpose of the drug and should be told
that it is not a truth serum and that it would not expose his or her secrets and
whether he or she states them unconsciously, they will be kept confidential. If
possible, a family member of suspect should remain present during the test.

ix. After intravenous injection of the truth serum the suspect should be involved
in conversation on unconcerned topics.

x. When the suspect’s speech began to slur, he/ she should be asked to count the
number backward from 100. When number begins to skip and intervals
between the two speeches become long, questions may be asked.
xi. Questions about known items and matters should be asked.

xii. The suspect should also be asked to review some pleasant memories from time to time. This is so that negative materials may be balanced and near experiences stored in suspect’s memory can be revealed.

xiii. After the procedure ends the suspect should remain on bed rest for about 5 hours.

**Success Rate of Narco-Analysis Test**

In assessing the credibility of the Narco Analysis, the Forensic Science laboratory, Bangalore reports that more than 300 people have been subjected to this test for committing various crimes in India. Out of this, the success rate of this test was about to 96-97 percent as evaluated by the investigating agencies. Moreover about 25 percent of the total numbers of individuals subjected to Narco-Analysis test were proved to be innocent. Thus the technique has been very helpful in crime investigation as far as India is considered. Moreover it has provided an alternative to public and human rights violation because of custodial violence.

**Critical Analysis of Narco Analysis Test**

Narco analysis may be used in medical realm for diagnosing mental debilitation among individuals. It is also used for restoring speech to mute persons, reviving memory in case of amnesia and for expression of suppressed or repressed thought or conflict. In criminal investigation, Narco analysis forms one of the important techniques for forensic analysis. In India, where custodial violence is very

---

widely prevalent, Narco analysis can act as non-invasive asset for investigation and for prevention of crimes and if used in a scientific way can be very useful for interrogation of the suspect. Narco analysis is very useful in investigation of cases of terrorism, organized crimes or trafficking where finding of evidence is a tough task. Narco analysis is also useful in saving the innocents from prosecution and eliminating the use of third degree method during police investigation. In addition, it can help in saving time in criminal cases leading to speedy and cost effective justice delivery.

However, it must be kept in mind that the test is not 100% accurate. Dr. B.M. Mohan, Director of FSL, Bangalore claims that Narco analysis should be discredited. Moreover the investigator can play false tricks with certain subjects making them record totally false statements. Since the cognitive faculties are suspended during the test, the subject is highly vulnerable to get trapped in biased attitude of the examiner. It is also very difficult to suggest an exact dosage of drug for a particular individual as it varies from person to person depending upon his physical and mental health. Sometimes administration of the wrong dosage may cost the subject his/her life also. The effect of these drugs could be very depressant over the cardiac, respiratory and excretory system of the body. At three to five times the sedative dose, the same barbiturates are hypnotics and can induce sleep or unconsciousness from which the subject can be aroused. In larger doses a barbiturate can acts as an anesthetic. In even larger doses, barbiturates cause death by stopping respiration.
Brain Mapping or P300 Test

It is most notable that Brain has been the centre of attraction for neuro-analyst for decades. It is centrally involved in every human action and records everything that human beings do, including criminal acts. Due to this reason the brain has been the key point in inventing all equipments of lie detection be it Polygraph or lie detection test, P300 or Brain Mapping or Narco analysis. In these, Brain Mapping is the latest and one of the most valuable scientific tools to criminal investigation. Also known as Late Positive Complex or P3 or P300, it was developed by Dr. Lawrence A. Farwell, Director and Chief scientist of ‘Brain Wave Science’ IWOA and a well known neurologist himself, in the year 1995. It measures neural responses exhibited after an object is shown to the subject or on external stimulus to the subject. Brain mapping is used to determine whether certain information is present in the brain of a person or not i.e. it is a scientific test by which guilty knowledge stored in one’s brain can be determined. Brain mapping thus matches the fingerprints of the information in the brain with that of actual crime scene.

In this technique, a preliminary interview of the suspect is carried out to ascertain whether he is concealing any important information. Thereafter sensors are attached to his head and he is made to sit in front of a computer. Here he is shown certain images and made to hear certain voices that has some links with the crime or crime scene. The sensor attached to head monitors and records electrical activity and P300 waves in the brain, which is produced only if the subject has link with the stimulus. No question is asked from the subject during this time. Thus Brain mapping matches the response of suspect’s brain to controlled stimuli of information relating to
crime and crime scene. In case the subject has no relation to the crime or crime scene, no P-300 would get registered during the test\textsuperscript{84}.

It is also a technique in which Indians too have contributed in its advancement. The problem in this technique, as devised by Dr. Farwell, was that it gave unreliable response when the suspect who while sitting before the computer screen presses the wrong button or does not presses any button at all. To meet this error, Dr. Mukundan of Brainex (Brain Experience) Company at Bangalore has designed special software called “Brain Electrical Activation Fingerprinting”. Another change is in the part of the brain from which the response is collected i.e. sometimes information is gathered from frontal lobe of the brain and sometimes from the posterior end under the modification. Highlighting the utility of the technique, it was once commented by Dr. Mukundan that “The technique is so specific that one can even find out how much money was paid to a contract killer or what called him up the day before the killing”

**The Science behind Brain Mapping**

Human Brain behaves like a black box in an airplane which has definite instinctive capacity to record person, events, places and objects etc as memories for a long time. These memories form the basis of scientific technique of Brain mapping as each memory is associated with a different response when stimulated by appropriate trigger of that particular memory. These responses are captured in form of electrical impulses on a machine called electroencephalogram with the help of electrodes strapped on the scalp of the person. When any information is given to subject which

corresponds to the information already stored in brain, it sends electronic signals and is recorded on this Electroencephalogram. Though the first electric current in a human brain was recorded in 1925, it was a group of 5 nuclear scientists led by Dr. Jerome Stowell who tried to unravel and register the wave length of these electric impulses or electrical waves. Since each person’s brain, being different, emits varied and distinctive wavelengths of electric impulses, each person’s brain wavelength can act like his/her fingerprints. But Dr. Lawrence discovered that P300 was a common single aspect of a larger brain wave response. If a person knows an event or object or an act and its visuals is shown to him, the P300 electrical brain wave responds to that fact or event. He thus patented it and named it MERMER response which stands for MEMORY AND ENCODING RELATED MULTIFACETED ELECTRO ENGEHALOGRAPIC RESPONSE. As being common, its inclusion in Brain Wave Analysis Algorithm has made it a definite determination in Brain Mapping Test. So unlike the availability of DNA & fingerprints in major crime scenes (which is 1%), the Brain Mapping test applicability in major crimes is 70%.

Brain mapping is thus a boon for investigating agencies in cases of planned commission of crime where the physical or biological evidences either are absent or are made to vanish by the perpetrators of the crime. The brain of the perpetrator is always with him while planning, and committing the crime. By this technique it is measured as to whether there is crime related information stored in the brain of the suspect or not. It can, in short, determine the presence or absence of a person at crime scene. It can also, depending on the information related to the execution of the crime, make distinction between witness and a perpetrator.
Brain Mapping – Modus Operandi

Equipment required for the test

The equipment required for a proper analysis of the subject in case of Brain Mapping includes:-

i. Personal Computer

ii. Data Acquisition Board

iii. Graphic card for driving 2 monitors from single computer

iv. 4 channel EEG amplifier system

v. A particular software of brain Fingerprinting laboratories

vi. Headband specially developed by brain Fingerprinting laboratories to hold electrodes.

In this technique, special electronic test sensors are attached to the scalp of the subject in the form of a special head band and the subject is seated before a computerized monitor. The sensors catch the electrical activity in the brain and record P300 wave, which is produced only if the subject has some correlation with the pictures shown to him and the sounds which he is made to hear. P-300 is an electrically positive component and has a peak literacy of about 300 to 800 milliseconds at the midline partial area of the head. The subject views, on the computerized screen or even directly, a series of relevant and irrelevant words, pictures, signs, phrases etc. and the test subject is called upon to press button on the correct option. The responses of the two different types of stimuli are measured to know whether the relevant material is known to the brain or not. Processing of known information relating to the crime deposited in the
brains is exposed by identifiable pattern in the Electroencephalogram outline. Thus the apparatus works not on emotions but on Cognitive Brain responses.

Technically explaining, Brain Mapping involves confrontation with a stimulus of special significance with electric signal known as P300 emitted from individual’s brain, beginning approximately 300 milliseconds after the confrontation. Since it is based on EEG signals and graphs, the system does not require the subject to speak at all and he in a way continues to exercise his right to keep silent. The suspect wears a special hair band with electronic sensor that measures the EEG from several locations on the scalp.

**Critical Analysis of Brain Mapping**

Although helpful and used by FBI to convict criminals, Brain Mapping cannot in any scenario distinguish the reason/motive behind a person presence at the crime scene. Also in certain crime like that of a person disappearance or in sexual assault case, Brain Mapping is useless as in the former the reality of whether any crime is committed or not is unknown while in the latter the question of intimacy being consensual or not cannot be proved by using Brain Mapping Test. This technique also cannot be used on mentally ill or heavily alcoholic suspect and may not be helpful in cases of habitual criminals.

The brain mapping analysis identifies only the existence or nonexistence of information related to crime and not the guilt or innocence per se. Such a proof produced by an expert can only supplement other evidences in a criminal
trial and impart a sense of totality to the investigation for the appreciation of the judge. It may be possible that in certain case, a person may possess virtually all the available information about a crime but may not be the perpetrator of the crime. In such cases the validity of the technique may result into counterproductive outcomes and can wrongly identify the perpetrator. According to Mr. A.A. Samdani, Ex Judge and Mr. Sharique Rizvi, Associate Prof. Indian Institute of Information and Technology,

“Information present in the mind does not always mean that suspect is guilty. It may be possible that the subject has been a witness to the crime or he or she has already read details in newspaper or seen in media which has been imprinted in his or her mind.”

The application of Brain Mapping as a forensic tool in individual cases will depend upon the genuineness of the investigation and other factors. The test would not be applicable in a case in which two suspects in an investigation were both present at a crime, but one was a witness and the other a perpetrator. The method can only detect information from their memory that would place both at the scene of the crime and it cannot decide what their roles were, thereby creating a distinct possibility of an innocent eye-witness becoming a suspect of the crime and giving a dubious opportunity to the real culprit to create a situation of doubt. Moreover, the method would not be definitive in a case where the investigators do not have sufficient information about a crime to be able to test a suspect for crime relevant information stored in the brain.

85 “Brain fingerprinting in forensic science”, available at : blogs.rediff.com (visited on date 28-02-2013)
This technique is also criticized on the ground that it is violation of brain privacy. By this a person loses his right to keep his thought to himself. This is also not useful in case of a person who loses his memory, e.g., old people easily lose memory and therefore the authenticity of brain mapping on an old man can easily be discredited. Similarly, a person suffering from deficiency in memory can exit normal P300 brain waves.

The six-member committee headed by National Institute of Mental Health and Neuro Sciences (NIMHANS) Director Dr. Nagraj concluded that Brain Mapping is unscientific and should not be used as a tool of investigation and evidence adduced through brain mapping should be made inadmissible in Courts. He also said there is requirement of a methodical, systematic and meticulous examination of the procedure as it lacks ascertained principles 86.

**DNA Profiling**

One of the most reliable technique of scientific aid in criminal investigation in 20th century has been DNA profiling. It is still most widely deployed tool for effective investigation and enjoys the confidence of judicial fraternity. DNA is the abbreviation of the term, “Deoxyribose Nucleic Acid”. It is an organic substance which is found in every living being and acts as his/her genetic blue print. DNA can be obtained from a wide variety of sources like, blood, semen, bone, saliva etc 87.

DNA was first discovered by Fredrick Mischer in the year 1869. Sir Alec J.

---

Jeffery discovered the use of DNA in forensic analysis in 1984 in England and it was first used in the famous *Endbury case* wherein two girls were raped and murdered\(^8\). Since then a number of techniques for DNA analysis have been developed by scientists making DNA profiling a quicker and cost effective technique for criminal investigation. Since DNA of every individual is unique (The probability of DNA being same is one in three billion), DNA profiling has turned out to be boon for criminal investigation in modern era. It is the most credible form of evidence as it cannot be easily tampered with. It is thus rightly termed as “*gold standard of evidence*” among the forensic fraternity.

Thus scientific aid like DNA profiling enables forensic investigation to identify individuals from their DNA sequence where the genetic pattern of the suspect is matched with samples of biological evidences ranging from hair, blood, skin, semen, saliva etc collected from the scene of crime to establish a credible link between the crime and the offender. Realizing this immense potential, the western countries have begun to utilize this technique frequently for solving complicated cases. DNA profiling being an authoritative technique is capable of distinguishing one individual from the other, with the exception of identical twins or clones\(^9\). DNA profiling is also being deployed in solving paternity disputes, solving cases of switched babies, in diagnosing inherited disorders and human diseases, in study of population genetics, for claiming of security benefits, for pedigree analysis of animals and for vegetatively grown and self-pollinated crops or plants in the agricultural areas\(^10\).

\(^8\) “DNA test and its relevance in forensic science”, available at: www.dnasourse.com (visited on 14-4-2012)
Thus the technique of DNA profiling offers a great deal of accuracy greater even than any of the currently deployed scientific methods as it allows examination of the human biological material at the most fundamental level i.e. the DNA molecule. The technique of DNA testing and its application in various fields and its use in identification of the accused are well established now across the world. It has lately emerged as one of the most useful and powerful methods of criminal investigation having great acceptance and objectivity in comparison to other scientific methods analysis.

**DNA Profiling - Modus Operandi**

A number of methods exist for preparing and analyzing the DNA which generally involves examining the non coding portion of DNA strands and genes which serve as templates for making proteins in the cells. The remaining part of DNA includes repeating base pair and sugar molecules. Different types of test are deployed to search and analyze different base pairs for identification of any individual for number of applications\(^9\). The various methods for DNA testing depends upon circumstances such as age, size and handling of sample etc and can be categorized into the following:

i. Restriction Fragment Length Polymorphism (RFLP) Method

ii. Polymerize Chain Reaction (PCR) Method

iii. Short Tandem Repeats (STR) Method

iv. Amplified Fragment Length Polymorphization (AMPFLP) Method

v. Y-Chromosome Method

---

vi. Mitochondrial DNA (mtDNA) Method

vii. Variable Number of Tandem Repeats (VNTR) Method

**Relevancy and Reliability of DNA Testing In Crime Investigation**

DNA technique is increasingly becoming important for ensuring the fairness in the Criminal Justice System all across the world. For instance, in 1999, New York authorities correlated a man through DNA proof to at least 22 sexual assaults and robberies that had terrorized the city. In 2002, authorities in Philadelphia, Pennsylvania, and Fort Collins, Colorado, used DNA evidence to link and solve a series of crimes (rapes and a murder) perpetrated by the same individual. In the 2001 “Green River” Killings, DNA proof made a major breakthrough in the sequence of offences that had lingered unsolved for years in spite of a large law enforcement task force and a $15 million investigation. In America, some criminals who have served over 20 years in prison or even those who faced death row for a crime they didn’t even commit have now been finally exonerated, thanks to new DNA test proving their innocence. DNA test undoubtedly can connect a suspect to a crime scene and help investigative agencies to find early conclusion to a criminal investigation. Similarly in the *Rajiv Gandhi Murder Case* in India, the DNA samples of alleged assassin Dhanu were compared with her relatives, which gave conclusive proof about her being involved in the gruesome attack. In the famous *Tandoor murder case*, the DNA samples of the victim Naina Sahni were compared with that of her parents to establish her identity.

---

92 “Importance of DNA testing in forensic science”, available at: www.whitehouse.gov (visited on 9-5-2011)
As far as the reliability of DNA as evidence is concerned, the technique has to pass critical test concerning the following:-

i. Timeframe

ii. Probability rate

iii. Error ratio

On the first account, DNA technique can be used for a longer period of time. There have been cases where the DNA analysis gave conclusive proof of the crime like murder even decades after the death of the victim. It also have high probable rate of certainty where there is very low chance of producing erroneous result. Moreover the samples can be first catalogued and then matched with the main sample to avoid any apparent error thereby reducing the error ratio drastically. With further aid from digital imaging, DNA is now proving more reliable and readily accessible where customized information can be provided to various State Law Enforcement agencies. As far as management of DNA database for ensuring reliability is concerned, there must be quicker analysis by weeding of searches where probable cause does not necessarily exist (Cold Searches) and giving importance to those where probable cause does exist (Warm Searches).

For further improving the reliability, a comprehensive legislation standardizing operational procedures and instructions for proper establishment of laboratories with state of the art equipment is the need of the hour. The legislation should also incorporate the manner of handling test samples so that the chances for error in the result can be minimized. It should also have guidelines for handling an
unfit specimen, if no other option is available. The legislation should also encompass a distinct code of conduct for effective crime scene management including careful labeling and handling of such test samples at the crime scene.

**Application of DNA Profiling**

Right from conviction to exoneration of crimes of varied nature, DNA has played a pivotal role not only in criminal investigation but also in criminal prosecution. Since the year 1986 when DNA analysis saw its first use in criminal conviction, hundreds of criminal cases have reached to its conclusion not only in India but also across the world with DNA profiling providing a concrete form of evidence. From a tiny drop of blood to the thin hair of suspect can now be utilized as a credible form of evidence in a criminal trial, if the technique of DNA profiling is used properly. In cases where the law enforcement agencies have reached a dead end, the DNA Profiling technique can help them in not only shedding new light to existing clues but also, in rare cases, solve them completely.

Nonetheless following are some of the prominent applications of DNA Profiling:

**Genetic fingerprints for identification**

DNA in human being carries the ‘‘blueprint’’ (genes) from which ‘‘building orders’’ for growth and maintenance activities for our body is transmitted. Except for identical twins, no two people have the same DNA. Since we all belong to same species in animal classification, large strands of DNA are same in all of us except the
small segment called as ‘Junk DNA’. It is this unique strand of DNA that is used by forensic scientists in criminal investigation through several chemical techniques like electrophoresis, radioactive DNA, and x-rays. The resultant characteristic pattern obtained is known as genetic fingerprint. Because different people have different junk DNA, the genetic print so obtained is a credible technique for identification of individuals for varied functions.

**DNA Parentage Testing**

Since every individual derives a set of genes from respective parents, DNA profiling can also aid in establishing biological parentage of a child. The test result can, however, provide a probability that a person is the biological parent of a child and, if that probability is sufficiently high, an inference of parentage may be confidently drawn. DNA parentage testing may thus be used to establish evidence in the circumstances where parentage is declined by the individual or an individual might seek parentage testing in order to obtain evidence of non-paternity for the purpose of civil proceedings against the child’s mother to prove “paternity fraud”. In mass disasters, such as, airplane crashes or natural calamity, DNA parentage and relationship testing is increasingly used in identifying human remains where the body of the deceased is no longer recognizable.

The scientific accuracy of parentage testing conducted by accredited laboratories has a probability of around 99.5% for finding the father of the child\(^9\). Though it has a high probability but still the social, psychological and economic

---

consequences of unreliable testing makes it imperative to maintain the highest technical, scientific and professional standards in conducting parentage testing in the country. It is thus often suggested that parentage testing be done under supervision of the courts to ensure both the accuracy and reliability of the evidence admitted. Possibility of `DNA fraud’ by laboratory staff in such test is a matter of grave concern and there should be a proper mechanism to address issues arising from the test results and for safeguarding and protecting the integrity of samples against tampering or deliberate fraud. The option of using court supervision would make parentage testing subject to a court order and would enable the courts to provide independent oversight of testing, including in relation to the validity of consent94.

The question of disputed paternity or maternity may arise in the following circumstances95:

i. Alleged adultery and suits for nullity of marriage where the child is born in lawful wedlock and the husband denies that he is not the father of the child and seeks divorce on this ground.

ii. Black mailing where a child is born out of lawful wedlock and the mother accuses a certain man as the father of the child but the man denies the accusation.

iii. Suits for maintenance of illegitimate children.

iv. When there has been an allegation of interchanging of a child with another in the maternity home or hospital.

94 Hardik Mehta and Rahul Desai,”Relevance of DNA as evidence from Indian perspective”,Gujarat Law Herald 21(2009)

95 Kishan Vjj and Rajesh Biswas, “Basic DNA and Evidentiary issue”, Jaypee Brother Medical Publisher (P) Ltd, New Delhi, 2004
v. In the case of kidnapped child, where the women who has kidnapped the child claims to be the mother.

**Forensic DNA in non criminal cases**

DNA analysis may be highly useful when a question arises in immigration cases, particularly when immigrants claim family relationships to United States citizens. In United States, DNA tests are often deployed in proving the biological relationships for the claimant on the insistence of immigration courts. Also using mitochondrial DNA method, forensic teams help in identifying the descendents of individuals. This was widely used in September 2011 plane crash with the World Trade Centre where victim’s forensic DNA tests were compared with his personal items such as toothbrushes and hairbrushes. Further researches in DNA analysis technology is undergoing in non-forensic fields such as medical research, genetics, or biochemistry.

**DNA profiling in the realm of Personal laws**

As far as Maintenance under Section 125 of Criminal Procedure Code\(^{96}\) is concerned, it requires a man to provide maintenance for wife, children (legitimate or illegitimate) and his parents. This has an added clause that such maintenance will only be provided when the maintainable individuals are unable to fend for themselves with proper care. However, often the defendant seeks to avoid providing such maintenance after terming his children as illegitimate (i.e. being born out of

\(^{96}\) Criminal Procedure Code,1973
adulterous nature or spouse paramour). It is here that DNA profiling help in removing the ambiguity before the court of law and thereby awarding maintenance in accordance with law. This would greatly avoid the misuse of law by such persons by finding loopholes. Although the test in such cases is voluntary as propounded by the law and established by various judicial decisions, need has arisen to make DNA test in such cases mandatory as the probability of tempering with the DNA samples is quite remote.

Similarly under Section 497 of Indian Penal code\(^{97}\), where adultery is punishable by the court in case a person cohabit with the wife of another person, the rebuttal of the husband to recognise the child born out of cohabitation can become a complicated issue as it is difficult to refute that the husband do not have access to wife during that time. Under such circumstances, the frustration of the husband could cause him to undertake any criminal act of serious nature extending even to murder or domestic violence. In such cases, DNA testing can be put to proper use and the legitimacy of the child may be ascertained in the womb itself or even after birth so that heinous crime may be avoided. Moreover if the legislature makes a law making DNA testing mandatory for the offences under this section, it can at least act as a deterrent for the woman who conceives from a person other than her husband.

In the same breadth, when the matter of inheritance comes before the court, DNA testing provides the most foolproof method to establish that whether a child is legitimate or illegitimate. However, lately the artificial insemination of a woman

\(^{97}\) Section 497 in The Indian Penal Code, 1860 “Adultery.—Whoever has sexual intercourse with a person who is and whom he knows or has reason to believe to be the wife of another man, without the consent or connivance of that man, such sexual intercourse not amounting to the offence of rape, is guilty of the offence of adultery, and shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both. In such case the wife shall not be punishable as an abettor”. 
using the semen of a person who is not her husband and without his consent has given birth to various legal issues. Inspite of the above, DNA profiling plays a predominant role in criminal investigation and conviction in the modern era.

**Critical Analysis of DNA profiling**

To obtain a higher proportion of certainty in determining the origin of the crime in an environmentally challenging crime profile, DNA is acts as an ultimate forensic tool. This biological based forensic tool generates a distinctive yet similar genetic pattern irrespective of the source from which it is collected. Ranging from semen to hard tissues, DNA is a powerful identification tool which irrespective of the environment remains stable for a longer period of time. Moreover, DNA is somatically stable. This, unlike the other markers, is a boon for the investigation agencies as despite the sample material getting degraded, it is possible to conduct DNA test time and time again, thus meeting the ends of the justice. A wide variety of evidences including even dried stains of blood and semen can now be collected without much fuss and tested to aid the court of law in punishing the culprit and reaching to an early conclusion of the trial. After the development of DNA profiling technique being adopted by the investigative agencies in a big way, the success rate of solving of difficult cases have been considerably increased.

However despite DNA profiling proving to be a useful tool in criminal investigation and prosecution, it cannot be always possible to conduct such investigations because the amount of DNA extracted may not be sufficient for testing. Furthermore, there has been considerable controversy about the use of DNA, the
statistical nature of the evidence it offers, and the validity of the testing. The critiques also argue that there is a lack of quality control standards among laboratories, most of being, where DNA testing is conducted. Lack of such controls, they contend, leads to many errors in testing as to invalidate any statistical evidence. Besides this, there are some technical problems with DNA as any scientific results cannot be 100% correct and backing of the scientific result by a wrong fact may end up into a wrong conclusion. There are always chances of mischievous acts on part of human agency in order to avoid the guilt. Thus, a DNA report should never be made as the sole basis to identify a person. This has also been enumerated by the judiciary time and again in its number of landmark decisions.

**Surveillance & Computer Forensics**

Modern day law-enforcement gives more primacy to crime prevention rather than fire fighting with the criminal activities. This is because of the extent of the damages which modern day crimes like terrorism, trafficking, and organized crime may cause to individual life and property as well as to the economy which may over the period of time acquire catastrophic proportions causing grave threat to national security and individual existence. Thus need is to pre-empt the complex criminal activities with proactive initiatives in which scientific aid like surveillance plays a pivotal role. Thus Surveillance is the covert observation of people, places and vehicles, which law enforcement agencies use to investigate allegations of illegal behaviour. This simple definition includes a plethora of techniques and methods that can be considered a form of surveillance. The most well known methods include stationary surveillance, technical surveillance (typically covert video or audio
recordings), electronic surveillance (digital observations, keystroke counting), and many more. Nearly anyone can engage in surveillance once properly trained and educated; individuals using various techniques of surveillance range from federal officials trying to save lives from terrorists and other criminals to private investigators gathering evidence for civil court.

However in the past decade, individuals, business houses and corporation have tendencies to carry out their activities electronically to a large extent and more prominently in the developed world. With the expanse of electronic realm in nearly every sphere of life, the amount of data in any format electronically is beyond any human comprehension. In this respect, electronic surveillance can become handy in alerting the law enforcement agencies of suspicious activities in this modern world.

Moreover the massive growth of internet in the last decade of last century had been heralding for carrying out wide spectrum of activities. Whether big large corporations or government, all are looking for potential data generated electronically for their own interest. It may be that large corporations may need this data for strategizing their business visions and policies while the government may tap in for this vast amount of data for securing their national interests. Thus the ends may differ but they all have lately realized the immense potential of the large amount of data generated and have engaged in electronic surveillance more comprehensively than ever. Though through electronic surveillance it is possible to gather information irrespective of time and place, it becomes a cause of concern when the same technology is driven against the state itself. A number of
methodologies exist for capturing data using electronic surveillance which are described briefly as below:

i. **Wiretapping:** It includes intercepting the communication with the help of electronic equipments placed between the communication channel of the stakeholders involved. It is also without the knowledge of the party involved in the conversation or communication.

ii. **Bugging:** It involves the placement of an external or internal electronic surveillance device which is miniature in its size near to the source of communication to be monitored. Unlike the wiretapping, bugging can overhear multiple conversations at the same time. However the effectiveness of the whole setup depends on the location of planted device.

iii. **Pen Register:** As the name suggest, it records the number of calls made from the device when it is placed on the telephone line. It is widely used by telecom operators for fraud detection. In fact information related to calls like call duration, call time and number are the only thing being recorded. A list of all calls can also be accessed by obtaining billing records provided it is under the post paid plan.

iv. **Video Surveillance:** It involves the use of close circuit television cameras for the purpose of video monitoring and sometimes recording of individual behaviour or action. It is mainly used to check threats but it can also be used to gather evidence in relation to a crime or a crime scene. It is emerging extensively as the technology across the world to monitor public places. Unlike the television broadcasting, video surveillance equipments transmit through point-to-point wireless links.
The surveillance cameras (CCTVs) are extensively used in United Kingdom where there are more than 42 million units installed. Even some Central Business Districts have been provided with cameras equipped with night vision and infrared capabilities. Entrance in central London, for example, is host to a security system which captures the photograph of the vehicle along with its number plate and driver through the CCTV. Such an arrangement helps not only in containing crime and increasing the rate of prosecution, but also instills a set of confidence among common citizenry about the capabilities of the law enforcement agencies. Another example is Singapore where CCTVs are deployed for traffic enforcement and bringing the practice of littering to an end. In India too, though in its initial stage, these surveillance activities are on a rise. Many important cities like Chandigarh have got CCTVs installed at every traffic signal to enforce the traffic regulation more efficiently. Private sector is much ahead in this endeavor as compared to the public sector which is still catching up. The latest use of CCTVs is in the form of a counter terrorism tool in which the entire city would be covered by the network of these equipments for monitoring of any subversive activity. London is one such city for such use of CCTVs. With added feature of face recognition this scientific tool is increasingly coming to the aid of intelligence agencies of the countries to identify potential culprits with nefarious designs entering the country. Moreover many of the international organizations are now realizing the potential of the video surveillance in keeping law and order across the cities under control and prevent untoward incidents from disrupting the peace and tranquility of the country. For instance, UNFICY (United Nation Peacekeeping Force in Cyprus) is monitoring the buffer zones on the island, 24 hours a day, through video surveillance. With the burst of new technologies like Thermal imaging, Motion detection, Passive millimeter wave technology etc,
video surveillance is emerging to be very handy to law enforcement and surveillance officials for ensuring safety and security to the common citizenry.

**Interceptions and Surveillance**

Interception refers to tapping of the communication network to overhear or to record conversations of the individuals or organizations within the framework of law governing the country. It is the most prevalent scientific technique for the government agencies not only to check corruption but also suspicious terrorist activities regularly for greater societal welfare. It is therefore a covert operation that is legalized by vigilant law enforcement agencies under the mandate of the law passed by the legislating authority. It can be both active and passive; the latter being used only to observe the flow of a particular data. Though interception can help immensely in criminal investigation and prosecution, many a times voices of concern regarding the infringement of the right to privacy of individual are raised. In India, the Home Ministry is in charge of electronic surveillance and dissemination of the data so captured.

With the arrival of digital age, revolutionary changes have occurred in the technique of interception. Exchanges by installing linked circuits for routings of audio signal are things of the past and modern day tapping is accomplished through a remote computer far away from the place of event. Sometimes, there is digital switching involved where by merely switching, the tab can copy digitized bits to an alternate line from where it can be retrieved at some future time. Such tabs are so well designed that it is very difficult to detect them by an ordinary user of the service.
Though the electronic surveillance was not deployed at a wide scale, things changed after 9/11 terrorist attack in United States of America. US government with a firm resolve to seek justice for the victims and strengthen their counter terrorism module, made use of this technique at a very broad spectrum. The US Congress too supported the government in this pursuit by passing the legislation for intercepting conversation even of civilians without the issue of warrant by the court thereby setting aside the arguments from preachers of free speech and privacy. Thus the impending threat to national security forced the government of the day to use this technique of interception in a big way. In India, however, the case is entirely different. The country has been facing security challenges including terrorism for a long time even before the American attack and thus provisions for interceptions with adequate constitutional protection have been provided in number of legislations. For instance, Director, Intelligence Bureau; Director, Narcotics Control Bureau; Director, Enforcement Directorate and Revenue Intelligence; Director, Central Economic Intelligence Bureau are authorized to intercept any communication under section 5(2) of the Telegraph Act. However, the interception should be done in the interest of:

i. Security of the country
ii. Maintenance of sovereignty and integrity of the state
iii. Maintaining public order
iv. Maintaining friendly relations with foreign states
v. Preventing incitement or commissioning of an offence.

98 The Indian Telegraph Act of 1885
In this context, despite being empowered by law under section 7(2) (b)\textsuperscript{99}, the government has failed number of times to frame any rules for regulating illegal interceptions by the officials. This is in light of numerous judicial interventions by the Apex court reminding the government to maintain a balance between the fundamental right of privacy and need for national security. It is not uncommon for government officials to abuse the power at their disposal for vested interest in modern day government which got highlighted in the recent \textit{Nira Radia} tape cases. 

Further, though these interceptions are not accepted as primary evidence in the court of law, these recordings are allowed to be taken as credible evidences in terrorist cases under POTA\textsuperscript{100} and UAPA\textsuperscript{101}. Although TUCCR\textsuperscript{102}, as the name suggests, prevents interception of unsolicited commercial communications by telecom companies to protect the personal privacy of consumer and TRAI\textsuperscript{103} regulates their functioning, it is still proving to be insufficient as technological hurdles and unframed regulations are lurking as a threat for consumer privacy. Similarly, with deeper penetration of the internet, new forms of crimes are surfacing posing a challenge to security agencies. Phising/Spoofing, Blackmail/Extortion, Accessing Stored Communications, Sports Betting, Electronic Harassment, Child Pornography, Prostitution, Criminal Copyright Infringement etc are some of the crimes causing sleepless nights to the law enforcement officials. Over all these, new field of warfare in cyberspace has emerged in which communication channel and critical installation are being targeted by sophisticated, trained professionals from a remote location. Thus interception of the communication channel including

\begin{itemize}
\item \textsuperscript{99} Supra 98
\item \textsuperscript{100} The Prevention of Terrorism Act, 2002
\item \textsuperscript{101} The Unlawful Activities (Prevention) Act, 1967
\item \textsuperscript{102} Telecom Unsolicited Commercial Communications Regulation), 2007
\item \textsuperscript{103} Telecom Regulatory Authority of India Act, 1997
\end{itemize}
electronic surveillance can provide solutions to this upcoming threat to the society at large.

Lawful interception of network with sound regulatory framework is thus becoming the need of the present society to empower the law enforcement agencies. The Western countries already have armed themselves with the regulatory standards like ETSI\textsuperscript{104} in Europe and CALEA\textsuperscript{105} in North America. These are just the building blocks to what appears to be a secure lawful interception system. The European Telecommunication Standard Institute based in France, for example, has three interfaces namely HI 1 (dealing with warrant information), HI 2 (dealing with intercepted information) and HI 3 (dealing with content of communication). Such interfaces provide ease of access to critical information and also deal with transferring of information to various law enforcement agencies. Also the procedures are audited at regular interval to align them with the technological changes in this modern world. In India, the IT Act\textsuperscript{106} was the first step in dealing with the lawful internet interceptions for security purposes. It not only addresses the need for a comprehensive counter strategy for cyber crimes but also provides for business friendly regulatory regime for e-commerce platforms.

Section 69\textsuperscript{107}, for example, give authorities the power to intercept any information irrespective of network resource in the country. Further, it is up to the

\textsuperscript{104} The European Telecommunications Standards Institute
\textsuperscript{105} The Communications Assistance for Law Enforcement Act, 1994
\textsuperscript{106} Information Technology Act, 2000
\textsuperscript{107} Section 69, Information Technology Act, 2000 - “Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is
Controller of Certifying Authorities to look and direct such interceptions. The norm here is similar to that of wiretapping i.e. for maintaining public order and upholding the security of state. The act also shifts the onus to users which mean that if a user fails to provide encryption key to the authorities, she/he may face a jail sentence of up to 7 years or fine or both. This is in accordance with Section 44 of the act. Similarly in order to target various cyber hub/cafes, where large population of citizen have access to different web portals, Section 80 was incorporated into the act which states that Deputy SP of the district can order search and can arrest suspects on the basis of suspicious conduct without procuring a warrant. Besides, censoring information on the ground of public morality and imposing penalties on publishing objectionable materials which are deemed to be obscene on the Internet, the act also restricts the free access of World Wide Web to the citizens in the interest of national security or to prevent incitement of any offence.

Later while keeping pace with the revolution in mobile telephony technology, the government enacted IT (Amendment) Act, 2006 to curb the misuse of the internet through the use of mobile internet. The government thus included a wide

necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.”
range of communication devices to make the regulation more comprehensive. Even the act included certain non cognizable offences under its ambit and gave authority to officials to check the content of one's communication devices irrespective of it being accessed in the privacy of the owner’s home or office. The investigative agencies are now vested with powers that infringes upon the right to privacy of an internet user. Although the Apex court has tried to contain the power of the investigative agencies by declaring Section 66A of the IT act 2000 as unconstitutional in the landmark judgement *Shreya Singhal v. Union of India*[^108], a lot need to be done to improve the procedural regulation of the government, even in the interest of nation, as it can be abusive in its nature towards the very people it sought to protect.

**Computer Forensics**

Unlike the last century where the crime was limited to physical world, the crime profile in the 21st century has taken a leapfrogging. With Information Technology revolution, the criminal activities have reached to cyber world causing a grave concern to the safety and security of the country in general and individual in particular. A number of crime and abuses which are now a day’s happening digitally are:

i. Cyber financial fraud

ii. Software piracy

iii. Leaking or Unauthorized disclosure of confidential information

iv. Online Viruses and Trojans

v. Pornography

[^108]: AIR 2015 SC 1523
vi. Hacking of Websites and Network server

vii. Identity theft

viii. Illegal distribution an accusation of international property

ix. Supplying a low quality IT products

The most notable characteristic of cyber crimes is the absence of physical evidence. On the other hand, the search of digital evidence requires a professional or an expert who is familiar with the digital terrain. Such expert may also assist the law enforcement agencies right from lodging of the crime with the police to the investigation of the crime and ultimately to the prosecution of the accused after the trial. The expertise of cyber professional is also very useful in the interpretation and preservation of the digital evidence. His/her testimonies in the court of law are also very crucial for establishing the nature and extend of the crime by the suspect.

However it is to be acknowledged that just like cyber crime is of varied nature, the cyber expert too has to be equipped with relevant skill for a particular crime. For example a database technician or software engineer/expert is a professional in tackling cyber crime involving software and financial frauds while a network engineer/expert helps in tracing anonymous online identities committing crime of sending threatening emails or launching a virus attack to destabilize essential online services.

Computer forensics, thus, is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics
is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

**Surveillance & Computer Forensics-Modus Operandi**

**Surveillance – Modus Operandi**

With the tools of surveillance, it is becoming increasingly possible to invade privacy without physical trespassing. Law enforcement agencies can now photograph from a distance, conceal microphones in tiepins, observe by closed-circuit television, tap telephone lines, pick up conversations in another room by the use of electronic devices, and determine the content of mail without opening it. The day is not far when a man can be kept under constant surveillance without his ever becoming aware of it. Thus surveillance includes observing a person's location, acts, speech or private writing without his knowledge. This surveillance can be of two types: *Stationary Surveillance* and *Mobile Surveillance*.

Stationary Surveillance includes most commonly the surveillance through micro-miniaturized devices called microphone and the surveillance through Telephone tapping. The microphone generally has a transmission range from 300 feet to 1000 feet and can be placed inside a telephone, a flower pot, a picture frame or in any other object in the room. These are wireless devices and have a built-in battery-operated radio transmitter. When entry into the room to plant the "bug" is not possible, a contact microphone can be attached to the opposite side of a wall in the room which picks and records the sound wave vibration striking the wall. Further if
the walls are too thick, a variation of the contact microphone called a "spike-mike" is used. The vibrations are transmitted through spikes (the size of a small nail) and then recorded. Similarly, the most common method for listening to both sides of a conversation is the telephone tap. Unlike earlier days, modern telephone tapping is done through an induction coil, about two inches in size, that is merely placed near the telephone and the voice signals are carried by the magnetic field and recorded in the receiver.

The Mobile Surveillance, on the other hand, involves three components: a surveillance platform, a power source, and a camera/recording device. The easiest and least threatening surveillance platform for mobile surveillance is a vehicle. Once the platform is established, the next step is to hide the power supply and camera/recorder components into the surveillance platform. The technical connections and preparations should be made covertly at some secluded location. The power source should be 12V DC. Intelligence about the subject and the purpose of the investigation must be used to determine the location of the camera. Knowing what must be obtained will determine the placement of the surveillance platform and the positioning of the camera for the right field of view. One can also successfully hide this camera in a coat, a box, or a pile of newspaper; anything within the vehicle that conceals the lens. The bigger the lens, the better one must conceal it while still allowing the lens to see through the concealment. Typical pinhole lens board cameras have a wide-angle field of view that would require very close placement of the platform to obtain any beneficial video footage. The better option is the use of a small C-mount lens security camera. The recording unit is most often a digital video recorder of 12 Volt.
Computer Forensics-Modus Operandi

Cyber forensic investigators typically follow a standard set of procedures. After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy. Investigators use a variety of techniques and proprietary software of forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation. But this is not as simple as it seems. For the cyber expert, extracting data is made harder by the criminals through the act of concealment. The processed data in form of information can be concealed in a number of ways namely Steganography (hiding data inside a picture or digital image), Cryptography (hiding data in encrypted form by using cryptographic algorithm), Using Virtual Memory (simulating extra RAM and hiding file in the expanded hard disk without the knowledge of the user), Cluster Space Technique (smallest block of data storage called file stack used to hide data), Tapping (tapping into the user by existing login session and hiding data by gaining a new login section after passing all authentication requirements), Polymorphism (hiding in the form of viruses and worms) and Renaming (secret information containing file is renamed into a normal common file type which can easily escape the vigilance or in some cases break the attention of the expert looking for the information).
Other than these the real world cyber criminals also undertake steps to clean the crime scene or to remove evidences of their involvement in it. This technique of dusting of their digital footprints and obfuscating incursions detection is termed as Anti-forensics. Anti-forensics can range from data destruction to use of sophisticated software to eliminate their cyber footprints. Cyber criminals use every kind of resource to destroy evidence of their personal involvement. Most common method adopted by cyber criminals for this is called Spoliation which refers to altering the data so as to render it useless for being used as evidence in a potential litigation.

Just like the Anti-forensic technique for the cyber criminals, the arsenal of the cyber expert who tries to counter cyber attacks is filled with sophisticated techniques to provide viable solution to the complicated problems. Some of the techniques deployed by the cyber experts to counter cyber crimes are:

i. *Cross-drive analysis:* A forensic technique that correlates information found on multiple storage drives and social networks to thread in a systematic and relevant piece of information.

ii. *Live analysis:* The examination of computers from within the operating system using custom forensics tools to extract encrypted file system.

iii. *Deleted files analysis:* A common technique used in computer forensics which involves the recovery of deleted files and reconstructing the physical disk image again to extract evidence.

iv. *Stochastic forensics analysis:* A method which uses stochastic properties of the computer system to investigate activities lacking digital error. It is extremely useful technique for investigating data theft.
v. **Volatile Data Analysis:** Conducting time-sensitive work for retrieving data stored in the RAM of the computer before the computer is switched off.

Though a lot of progress has been made in the field of computer forensics, certain areas are still in the phase of infancy (lack of standardization) such as Software Piracy investigation. It is quite extensive and its investigation demand a greater expertise going into the complex logic of programming in the software which can search for a common trait existing in all prevalent programs. For example, all the downloading assistance software will have the same mechanism for cache of a file irrespective of the source. To conclude that a pirated version exists, the expert has to prove that although the mechanism for cache of a file looks same, the programming language must differ to qualify as distinct and innovative software. Similarly, it becomes more difficult for the expert if the programming language is different but algorithm of the original and pirated version is the same. In this case the expert has to break the programming code to verify the claim which becomes a more tedious task.

After analyzing the cyber crime, the expert has to prepare a report in which the technical details are provided for defining the nature of the crime, extend of damage which may help in conviction. Such reports ought to be help the judiciary in resolving their stand on the matter. However, this itself is a complex task as the report has to be prepared in such fashion that makes it convincing for non-technical person. Also as the cyber professional is not trained in legal knowledge, it is difficult to determine which point to stress upon while preparing the report so as to create a legally sound technical report.
Critical Analysis of Surveillance and Computer Forensics

Computer forensics is the modern counter strategy for increasing hi-tech crimes involving Corporate fraud, Intellectual property disputes, Digital theft, Breach of contract and asset recovery etc. Moreover Computer forensic analysts undertake their investigation in such a way that the electronic evidence becomes admissible in the court of law. However this field is relatively new and generally criminal matters are usually dealt with physical evidences. This makes electronic evidence something very new which are taken with a pinch of salt by the judicial mind. Fortunately it has been a helpful tool wherein important data needed for a case has been lost, deleted or damaged and has to be retrieved.

The main advantage of Computer forensics is its ability to search and analyze a mountain of data quickly and efficiently. They can search keywords in a hard drive in different languages which is beneficial since cyber crimes can easily transcends the national boundaries through the internet. Also the valuable data that has been lost and deleted by offenders can be retrieved which becomes substantial evidence in the court of law.

However the first setback using electronic or digital evidence is making it admissible in court. Since data can be easily modified and court requires evidences that prove the guilt beyond reasonable doubt, the computer forensic analyst must show to the court that the data has not been tampered with which is a tedious task to accomplish. Other disadvantage is the cost of retrieving data. Computer forensic experts are hired on per hour basis which becomes a costly affair. Moreover the
analysis and reporting of data can take as long as 15 hours depending upon the nature of the case. This becomes a problem as modern day courts do not have so much time to devote on a single case. Another drawback is that while retrieving data, analyst may inadvertently disclose privilege documents which may cause serious damage to the party to the case. It is imperative that the legal practitioners involved in the case must also have knowledge of computer forensics. If not, they will not be able to cross examine an expert witness. This also applies to the judge who can appreciate the utility of the evidence only when he/she has sound knowledge of digital forensics. The analyst too must be able to communicate his findings in a way that everyone can understand.

There are also reports which present a bleak picture of video surveillance system too. The United Kingdom Home Office Meta study and its systematic reviewing had concluded that instead of CCTV, street lighting is far more effective deterrent of the crime. In fact the study conducted by an University in UK suggest that even in areas where CCTV appears to be effective, the crime rate and video surveillance do not have a direct relation. As the report further suggests that the decrease in crime rate was due to the displacement of the crime to another area and to say that video surveillance had a part in it would amount to overstretching the facts. The Australian Institute of Criminology 2003 report\textsuperscript{109} also yielded similar results. It should also be put to note that law enforcement agencies of number of US cities like Oakland and Miami have abandoned camera systems because of its systemic failure in bringing down the crime rate.

Even in London, christened as the most ‘watched-city ’ of the world, the vast deployment of CCTVs could not deter nefarious plans of carrying out terrorist attacks on July 7, 2005 killing nearly 700 people\textsuperscript{110}. Although CCTV footage later helped in identifying the accused of such bombing, they certainly do not deter these anti social elements in carrying out these preposterous activities.

Although computer forensics has its disadvantage, the use of computers and the rise of cyber crimes call for an equally high end method of stopping it. The importance of surveillance and computer forensics can be gauged from the fact that December 24 every year is celebrated as World Surveillance Day\textsuperscript{111} by the international coalition of artists, scholars and others.

\textsuperscript{110} Michael Ray,“ London bombings of 2005”, Encyclopedia Britannica, Inc, September 27, 2013
\textsuperscript{111} Sally Ramage,”Privacy-Law of Civil Liberties”, iUniverse, Inc. New York Lincoln Shanghai, 2007,p 76