Impact of Technology in Investigations: The Judicial Response to Admissibility of Evidence Obtained Technologically

Ms. Jaisy George[*], Dr. Ashish Deshpande[**]

* Research Scholar, Symbiosis International [Deemed] University

** Assistant Professor, Symbiosis Law School Pune, Symbiosis International [Deemed] University

Abstract

Technology has aided the law enforcement agency with powerful tools for detecting and deterring crimes. However it has considerably eaten away a substantial part of the individual's liberty and privacy. This leads us to one of the major controversial issues of almost all the criminal justice jurisdictions across the world today: the admissibility of the evidences so obtainedviz., illegally,or rather 'technologically' curtailing the privacy of the individuals through the application and administration of the advanced tools and devices on the people.

The authors through this paper depict the scope and application of technology in crime prevention, crime detection and subsequently in the collection of evidence. The authors thereupon pin point their research to some basic issues of concern like, whether with the aid of new technologies available today privacy protection has been eroded in favour of the law enforcement? Whether the shift towards technology and the tools and devices borne out of it at the hands of the investigation agency has undermined the basic rights of individuals like privacy and personal liberty?To what extent do the exclusionary rule and the exclusionary discretion fit to the contemporary world?Is there a need for rethinking the legalprotections in the new technological era? etc. Then the authors proceed toevaluate how far the Indian judiciary has appreciated such evidence by availing the common law judicial discretion, as there is a legislative vacuum in this area.The paper thereupon attempts to closely analyse the important case laws in this area to ascertain the parameters taken into consideration by an Indian judge in dealing with the admissibility of technologically obtained evidence.

Keywords: Illegally obtained evidence, Technologically obtained evidence, Improperly obtained evidence, Exclusionary discretion, Right to privacy and personal liberty in surveillance, Illegal search and seizure, Technology in investigation, Admissibility of evidence in India, Judicial approach to admissibility of evidence.

1. Introduction

New technologies have without doubt enabled us doing things easier, faster, or more efficiently than ever before. And in some cases it has even made the once impossible, possible (Webster's Collegiate Dictionary, 9th ed., 1983). No different is the case of crimes and crime-commissions. In fact it would be no exaggeration in saying that technology has redefined the form of crimes and their commissions, particularly their modus operandi. The accused now-a-days are well informed and more educated and use sophisticated weapons and advanced techniques to commit the offences ending up in the enlargement of the old categories of crime, or popping up of 'new-crimes' (Joseph F. Coates, 1972). It has consistently changed the style of crimes and has generated new opportunities for crime. Thus it is true to say that technology has redefined the forms of crimes and the way in which it is planned and worked out *viz.*, organised crimes, terrorism, smuggling or other economic crimes.

Technology also leads to the concealing of information which would have been revealed in the past, without leaving any single trace of evidence (Orin S. Kerr, 2004).There is a version suggesting that, these instances of the present-day crime commissions no matter in whichever jurisdictions they fall, in order to control them if not to prevent them, policing also employs an equal share of high-

handedness in technology. The law enforcement agencies also need to adhere to the same technology and its' products *viz*., the devices that bring the crimes to limelight through evidencelike the electronic evidence, digital evidence, etc., for booking the offenders. The proponents hold so for the simple reason that they believe that the existing procedure and the use of traditional investigative techniques seem to be inadequate in such cases of newer crimes (Lucyna Kirwil, 2004).

2. Use of Technology in Investigation and Evidence

Yes, technology has been proved to be having an enormous enabling potential for detecting and solving crimes these days. Say for example the DNA forensics, DNA typing, fingerprint matching techniques etc. (Bert-Jaap Koops, 2009). These undoubtedly unfold newer prospects of data gathering and enabling profiling which could not only cater to crime-control but also enable crime prevention.It increasescompetence in policing too (Peter K. Manning, 1992). It provides that information to the officers which would not have otherwise been available to them by making use of the conventional investigative procedures (Dengke Xie, 2021). Even small police departments now routinely obtain location information, text messages, and other data from cellular carriers. Providers of Internet, email, cloud-storage, and social-networking services also provide sufficient information. The use of electronic devices to collect evidence relating an offence and to keep watch over a person has also found a place in policing. This also has got the capacity to keep a check and detect crimes and also to collect dataon suspicious persons and institutions. New surveillance techniques ranging from wiretaps, bugs, pen registers, photographic surveillance, wired agents and informers have occurred in recent times (Willie J. Elder Jr, 2007). Video recordings are also availed and obtained by the law enforcement agencies today which will include among it the surveillance tapes. And not to mention about the present day electronic devices now available to the eavesdropper-investigatorto collect information which are simply numerous. In reality therefore, electronic-surveillance provides for gathering information ofpersons any time and for any duration and that too without the knowledge of the individual under check.

Data obtained from digital media and internet usage also require a considerable mention here as it yields significant investigative leads to the officers. Such electronic communications made available from the internet and mobile phone service providers and the suspect's or victim's computers remain intact any time even after a long time of crime commission. Such an examination of the said electronic media could even reveal the ownership related data,deleted or even hidden orconcealedrecords,their internet activities etc. which provides the investigation agency with the ample lead.

Cellular tower information are also at aid to the investigation agency which gives significantdetailswith regard to the preciselocation of the mobile phone and thus effectively track his location; the movement of the persons or objects. Such tracking systems include in it the following: GPS which couldascertain the exact position of the object being tracked, Directional Find (DF)/ Radio Frequency (RF); Access-Control Systems, etc.

The other devices available for the investigation or the law enforcement agencies are: the answering machines and voice mail systems; the caller ID devices; cell phones; computers; customer or user cards and devices; web cameras, closed circuit television (CCTV) cameras and digital security cameras; facsimile; Global Positioning System devices; internet tools; keystroke monitoring; Personal

Digital Assistants (PDAs); sniffers; vehicle black boxes and navigation systems etc.

3. The Issue with the Evidence Obtained Technologically Unveiled

However it is a bare reality that the adoption of such scientific devices in investigation has delved into placing the individual under broad physical, psychological, and data surveillance. Here the authors refer to the evidence procured by phone tapping, compelled narco-analysis, illegal search and seizure, activities recorded by secret cameras etc. (Bharat Chugh, Taahaa Khan, 2020).It is also claimed by at least a few that such techniques step into the privacy rights of the individuals which lately has gotten the status of fundamental right as declared by the Indian Supreme Court in K. S. Puttaswamy v. Union of India, 2017. The Apex Court in this case has held that the right to privacy forms an intrinsic part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India (Bharat Chugh, Taahaa Khan, 2020). And hence it is widely opined that such procurement of evidence interfere the privacy rights of the individuals and thereby the fundamental rights deeming the procurement grossly illegal.

The moot question therefore is whether with the aid of new technologies available today, privacy protection has been eroded? Whether the shift towards technology and the tools and devices borne out of them has undermined the basic rights of privacy against unreasonable searches and seizures and personal liberty of individuals? It is true that the criminals and the potential criminals when get on to use and avail technology for crime commissions the investigation agency should also be given the same chance. But at what cost? Could the State undermine the privacy rights of its citizens for ensuring security? It is here that the authors raise their concern as to what extent the government, in the form of the investigation agency can pierce into the privacy rights of its' citizens?; To what extent do the exclusionary rule and the exclusionary discretion hold good in the contemporary world? It is significant to note here that some of the common law countries like the U.K. and India, has been practising exclusionary discretion, in dealing with questions regarding whether to allow such illegally obtained evidence in the court of law, unlike the American position of exclusionary rule which blatantly excludes the admission of any illegally obtained evidences as there exists a constitutional guarantee against the same arising from the Fourth Amendment.

There is no doubt that all the devices mentioned hereinabove helps the police in detection and the prevention of crime. The moot question here is whether the right to privacy of the citizens is at stake in such an instance; whether under the present constitutional interpretations and the statutory safeguards, the right to privacy can sufficiently be protected? Whether the traditional exclusionary rule and exclusionary discretion do no good in the contemporaryworld when dealing with evidence obtained technologically.

Justice Douglas rightly feared the situation (Osborn v. United States, 1966): “We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government.”

“The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge,” concluded Justice Clark a year later (Berger v. New York, 1967).These renowned judges were without doubt referring to the impact of science and technology in criminal justice administration and its impact on the citizens’ privacy rights way back then.

The questions of concern hence are, whether with the aid of new technologies available today, privacy protection has been eroded in favour of the law enforcement? Whether the shift towards technology and the tools and devices borne out of it at the hands of the investigation agency, has undermined the basic rights of privacy and liberty of the individuals? Is there a need for rethinking the legal protections in the new technological era?

4. The Value Choices to be Ascertained while Admitting Technologically Obtained Evidence

It is well established that the government agencies are not to intrude upon the individual's personal liberty and privacy unreasonably without any plausible cause. But facts reveal that the instances of present-day crime commissions require the policing also to avail the same technology. Hence on one hand the criminal justice scheme senses the necessity of taking aid of technology in stopping the ever-rising crime commissions, while on the other it upholds and respects the right to privacy and personal liberty of its subjects. How does the legal system balance these two opposing aspects and further justice?

It is well-settled that in common law countries all relevant pieces of evidence are admissible in the court of law, unless they fall under the category excluded by law, or is held to be excluded by exercising judicial discretion. It is relevant here to note that the word, 'relevant' is used in the legal perspective *viz*., it must pass all the tests of relevancy as prescribed under ss. 5-55 of the Indian Evidence Act, 1872 as far as India is concerned. Once the evidence gets into such a legally excluded category, they are accredited inadmissible irrespective of the other factors favouring its' admission, like the surfacing public interest demanding conviction of the accusedby applying the "fruits of the poisonous tree doctrine" (Talha Abdul Rahman, 2011). As is well established, the theory underlying this doctrine is that the original act of collecting the evidence by the investigating agency being improper or illegal as the case may be, will tend the fruits of the procurement also illegal.

In dealing with such illegally, improperly and irregularly obtained evidence and its admissibility the United States followa compulsory exclusionary rule. Exclusion of unlawful evidence is not subjectto discretion there, but a mandate of law. It is because of the fact that such an exclusion in US is not by reference to any ordinary statutory law or fairness, but to the constitutional law of the land viz., the Fourth Amendment to the US Constitution (Lindsay Freeman, 2021). However the basic problem of such a mandatory exclusionary rule is that the otherwise relevant evidence is suppressed and rejected from the trial proceedings (Hanna Kuczynska, 2021). It is to be noted here that mostly such an exclusion happens due to the non-compliance of the hyper technical application of the rules of criminal procedure. This means that 'proficient' criminal activity is benefitted. Which in turn suggests that the law enforcement becomes discouraged in attempting to deal with such organised crimes. Whereas in the other common law jurisdictions like that of India, such pieces of evidence obtained illegally or improperly are excluded by exercising the judicial discretion, the tool every common law judge is empowered with.

Time has proven that there is no easy solution to the problem posed by such novel-crimes and the crimes committed with the aid of advanced technology. New kinds of crimes without doubt seem to demand new law or legal regulations, or at the least cause the courts to rethink the way the relevant legal principles and doctrines ought to be applied to the new technologies. Or put in other words the courts are required to determine how the existing criminal law principles and doctrines could

effectively be applied to the new crimes and crime commissions. But interestingly, courts do not seem to have a common grounding upon the weightage of the evidence so obtained when exercising the common law judicial discretion. There is no clear-cut formula as to what is to be done with regard to its admissibility. The courts at times are found to be reluctant regarding the emergence of new technologies in investigation rendering the evidence so obtained inadmissible. It is so for the simple reason that the procurement goes against the age-old-conventional doctrines, read without any innovative interpretations. Or else the courts are seen manifestly admitting the evidence stating that the exclusionary rule and the discretion do not fit itself well in the technological era.

It goes without saying that technologies which were non-existent when the law was framed hold the actual challenge here. Say for example the US Constitutional law which calls for protection against unreasonable searches and seizures but not for any other newer versions of conducting surveillance. The Fourth Amendment to the US Constitution reads as, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”It is evident that this protection ought to change as per the changing circumstances and needs. The US Supreme Court has also opined so when dealing with it in a case. “It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology”(Kyllo v. United States, 2001). And this common sentiment is shared by all the systems today (Thomas Fetzer, 2012). The authors feel that as long as there are no statutory backings affirming it, an effective positive judicial intervention could be the only possible solution.

Therefore it is clear that the criminal justice systems across the globe ought to sacrifice some of the protections which centres on individual rights and individual liberties for the common societal interests especially in this era of technological advancement. This could obviously be done by means of a sound judicial process with the aid of common law judicial discretion (Morris Ploscowe, 1963). It is proposed that in order to admit the technologically obtained evidence an innovative interpretation of the age-old proven doctrines is required. Some hard thinking and realistic examination must be made in the current running rules of evidence and criminal procedure of the respective jurisprudence in order to find out the apt formula to guide these systems (Jerzy Skorupka, 2021).

5. A Quick Glance through the Judicial Decisions on the Admissibility of Evidence Obtained Technologically

When examining the judicial decisions and thereupon the courts' attitude on the use and impact of technology on privacy rights and individual liberties, which other country would be much better to be cited than the U.S., which is both technologically advanced for having been using all kinds of the above-mentioned tools and devices in their investigation procedure, and simultaneously has the constitutionally guaranteed protection against unreasonable searches and seizures?

In the context of the Fourth Amendment to the U.S. Constitution, the use of technology is found to disturb the general norms of policing due to its privacy-intrusive implication. The new investigative techniques being more invasive of the individual rights. There are many examplesone of which is the case of California v. Ciraolo, 1986. The Court here considered aerial watch by airplane and its implications on the Fourth Amendment. In this case, the investigators made use of an airplane to check whether the defendant grew marijuana in his backyard. The facts suggest that the yard was

surrounded by double fences ensuring any physical entry impossible. With the help of the airplane, the police could examine the plantations without actual physical interference. The Court maintained that the surveillance was not in violation of the defendant's property rights as the airplane was flown in the public airspace.

A similar stand was taken in United States v. Jacobsen, 1984 while considering whether chemical tests performed to detect the presence of illegal narcotics was violative of the Fourth Amendment. The Court here held that the defendant's reasonable expectation of privacy is not violated by means of such tests for the simple reason that cocaine ownership itself is illegal (See also Warden v. Hayden, 1966). When the defendant cannot have a legitimate claim over the illegal activity of owning or holding cocaine, a test to ascertain the presence of the same cannot be violative of his expectation of privacy.

No different was the approach of the Court when relying upon the records derived from the telephone and the internet. Court here again held that the Amendment does not forbid the information obtained revealed to a third person although there is a confidence reposed on it that it will not betray (United States v. Miller, 1967). The third person here being the new communication technologies like the ISPs or the cellular service. Hence it could be read in as once a person divulges data to the provider he is deemed to renounce his Fourth Amendment protection.

Another notable area to analyse the judicial reaction regarding the interpretation of Fourth Amendment on the adoption of technology by the police is 'electronic eavesdropping'. Say for instance looking into its evolution which begins in 1928 from Olmstead v. United States, it was held that telephone wire tapping by federal agents without trespass is not violative of the Fourth and Fifth Amendments. Chief Justice Taft holding in majority has limited the extent of the Fourth Amendment stating that there must be a trespass so as to be a violation of the Constitutional provision. "The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants". (Olmstead v. United States, 1928).

Thus summarising, the US Courts have been constantly and more progressively tackling the issues related to accommodating the Fourth Amendment to the contemporary technology. Some judges are seen simply rejecting the analogies of technologically obtained evidence to the literal search and seizures as referred to in the law, when the fact remains that there is no much conceptual difference in either of such searches (Thomas K. Clancy, 2005). In other words whether the long-established Fourth Amendment principles are to be rendered to the search of electronic evidence is nevertheless a matter of great concern.

Stepping on to the Indian jurisdiction in this perspective, the authors feel that, the first and the foremost parameter for an Indian Judge, while exercising the common law judicial discretion is the test of relevancy (Khagesh Gautam, 2021).Before we delve into the judicial approach to the admissibility of technological evidence, let us take a quick look at the Court rulings on the general admissibility of evidence. Here we put in the ratio of the Supreme Court decisions which cover the issue of admissibility of illegally, improperly and irregularly obtained evidence. The Courts are seen

to unanimously proclaim that the test of admissibility depend solely on relevancy, and save there is an express or implied bar in the Constitution or any other law, evidence procured technically or even illegally, is not liable to be shut out; (Nathooni Singh and etc. v. State of Uttar Pradesh, 1994); and that the admissibility of any evidence has to be ascertained considering the provisions of the Indian Evidence Act, 1872 (Inspector of Police &Ors. v. N.M.T. Joy Immaculate, 2004). The Courts have occasionally ruled that they are to scan the evidence so obtained with care and caution in order to be admitted in evidence and to be relied upon (Khet Singh v. Union Of India, 2002; State of Himachal Pradesh v. Shri Pirthi Chand and Another, 1996; John Ohuma Ogmekwe and Another v. Intelligence Officer Narcotic, 1998; Chinta Devi and Ors. v. The State, 1997; Sule Kareem v. Asstt. Collector of Customs, 1998). In another instance, relevance and genuineness was held to be the weighing standards for appreciating evidence so obtained. It was also declared in another case that if the relevance and the genuineness were proved then merely the fact that it was procured improperly would not bar its admissibility if it is otherwise relevant. (Magraj Patodiav. R.K. Birla, 1971). The court thereupon added on stating that the search and seizure provisions of the Code of Criminal Procedure provide the basic guidelines, but even if there are any violations to it, the court can admit the evidence.

Now let us look into the judicial reaction of the Indian Courts while deciding on the admissibility of technological or scientific evidence. Starting with the admissibility of a tape-recorded conversation.
In Yusufalli Esmail Nagreev. State of Maharashtra, 1968, tape-recorded conversation wasallowed as evidence. Here analogy was drawn to photographic evidence. It was observed that when a photo taken without the person's knowledge can become admissible, so is the case of a tape-recorded evidence which carries conversation unobserved by the speaker. This decision was deeply influenced by R. v. Maqsud Ali, 1966 wherein even incriminating tape-recorded evidence was allowed in evidence.

Later in R. M. Malkani v. State of Maharashtra, 1973 which discussed the same issue was to ascertain whether a person could be prosecuted upon incriminating telephonic conversation which was recorded by the police authorities. The parameters looked into by the Apex Court while appreciating the evidence were, firstly, whether the conversation is relevant to the matter in issue? Secondly, whether the voice could be identified clearly? Thirdly, check the accuracy of the recorded conversation.Here the method of procurement of evidence was actually appreciated by the Court describing it as a mechanical eavesdropping device. It held that that was merely a mechanical-involuntary process as there was not any element of coercion or compulsion involved.It clarified the position stating that a contemporaneous tape recorded conversation is definitely a relevant fact and is admissible as res gestae under Section 7 of the Indian Evidence Act. It added on ruling that such a tape recorded conversation is a relevant fact and henceadmissible as per Section 8 of the Indian Evidence Act.Here the evidence was considered at par with a photograph containing appropriate information and hence was declared relevant and also admissible. Adding on to it the Court emphasised that there was neither any interference in his privacy as such, nor any subjection to duress which would affirm the verdict. However it was suggested that such methods ought to be availed very rarely, with due care and caution.

Movingahead, let us now consider the cases involving telephone tapping as relevant piece of

evidence, in S. Pratap Singh v. State of Punjab, 1964, the Apex Court had approved in evidence the tape-recorded telephonic conversation. Here a conversation between a doctor and the CM's wife was allowed in evidence. It was used to corroborate the testimony of witnesses who had testified about such a conversation.

In another case, the telephonic exchanges intercepted in violation of the Telegraph Act, and the guidelines prescribed by the Apex Court in PUCL case, 1997 were held admissible in evidence (Dharambir Khattar v. Union of India, 2013). In the PUCL case, telephone tapping was held to be invading the right to privacy of an individual. The court ruled that privacy right which could be read in as a fundamental right under Article 21 of the Constitution of India cannot be infringed except by a procedure established by law (Sougata Talukdar, 2019). In the wordings of the Apex Court,

> ..the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy'..

In yet another case N. Sri Rama Reddy v. V. V. Giri, 1970, also known as the Presidential Election case, it was contended by the petitioner that one Jagat Narain sought dissuading for not contesting in elections. Their telephonic conversation which was tape-recorded was produced before the Court.Here the Court availed the conversation stating "witness might be contradicted when he denies any question tending to impeach his impartiality" and hence held that it can become prime evidence for which has been conversed and got recorded. Vineet Kumar v. CBI, 2019 dealt with the similar issue of whether the orders instructing interception of telephone calls violated the fundamental rights of the accused. The Bombay High Court deciding the matter held that a consequentialist approach will not lie good here. If every time such an 'end would justify the means'is approved for collecting evidence against the accused then it would indirectly mean that every other Supreme Court ruling could be evaded as also the mandatory statutory rules. It would hence end up in gross arbitrariness and blatant disregard to law procedures. Stating thus the Court has rejected the illegally obtained evidence, setting aside the interception orders and instructing the destruction of copies of intercepted messages.

As regards the admissibility of the findings of the truth machines like narco-analysis, polygraph etc. the Supreme Court judges again have mixed reactions. Such deception detection techniques has no evidentiary significance as was held in Selvi v. State of Karnataka, 2010. It was held that these techniques although seems to find the truth behind the case injures Article 20(3) rights of the accused (Bharat Chugh & Taahaa Khan, 2020). Therefore the Court has allowed such tests to be done only with the consent of the subject concerned. Ever since India has been using such techniques in a series of infamous cases like the stamp paper scam case, 2003; Nithari serial killing case, 2006;Arushi- Hemraj case 2008, Vyapam case, 2015 etc. However the evidence so obtained was deemed to have limited probative value in the trial proceedings. The admissibility of such deception detection techniques were to be tested on the touchstone of validity and reliability of it to the fact in issue (BartlomiejKrzan, 2021).

On dealing with the admissibility of DNA test in a murder case the Apex Court had admitted it in evidence (Narendra G. Goel v. State of Maharashtra, 2009). The test was used to ascertain the murdered woman as well as the accused. The Court here held that the acceptance of the test in evidence does not prejudicially affect the rights of the accused (Veena Nair, 2018).

Lately interviews given by the accused in TV channels are also taken as evidence in Courts. In Sajidbeg Asifbeg Mirza v. State of Gujarat, 2006, the prosecution requested the trial court to send forthe videographer as a witness in order to establish the contents of the interview made by the appellant. The counsel of the accused but objected this contending that those are simply extra-judicial confessions which was before the media and hence cannot be admitted in a criminal trialas evidence.The court however disagreed this prayer and called for him as witness to give his testimony. The Court so observed, “It appears that, no principle has been laid down by Hon'ble Supreme Court, but, it appears that, Hon'ble Supreme Court has observed that, if a statement is made in the course of an interview prearranged by the police, no weightage can be given to it at the time of appreciation of evidence. It appears that, there is no question of appreciation of evidence, but the only question to be decided is whether the grievance which is sought to be adduced by the prosecution is relevant or not? And whether the prosecution can be permitted to adduce such evidence or not?” Mirza appealed the High Court on the same ground which approved the Trial Court’s ruling. On further appeal, to the Apex Court on this point, the petition got dismissed on merits; holding that the statement made to the media by the accused can be considered relevant and admissible.

With regard to the admissibility of electronic records, the Indian Supreme Court in Anvar P.K. v.P.K. Basheer and Ors., 2014 has held that electronic records like, VCD, CD, chip etc. must be duely authenticated. Here the Appellant who had lost in the Assemble elections contended that the respondent had made defamatory matter against him in CDs as songs etc. The Court here ruled that such a record must be submitted along with Section 65-B certificate otherwise which the evidence would be inadmissible.Thus this case has made Section 65-B compliance mandatory for those who rely on records like websites, e-mails, etc. to be presented in evidence before trial courts. This was so declared to ensure authenticity and credibility as these records are more prone to alteration or tampering (Tejas Karia, 2015). Therefore an electronic record submitted without this compliance would be deemed to the status of illegally procured evidence resulting in its inadmissibility. By this landmark judgment the Supreme Court has in fact overruled Navjot Sandhu, 2005 which had permitted admission of electronic record without authentication as prima facie evidence (Ashwini Vaidyalingam, 2015). The latter case had actuallydealt with the admissibility of records of telephone conversations. As a matter of fact the lower judiciary in India seem to be indifferent about the authenticity issues while appreciating electronic evidence. And for the same reason they are seen admitting them even without complying the mandatory procedure laid down under Section 65-B of the Indian Evidence Act. Ratan Tata v. Union of India, 2010 was also one such case wherein a CD was accepted in evidence which was not in compliance with the evidence law mandate (Tejas Karia, 2015).

The literature available in this area highlight the arguments raised for and against the tilt of the

courts with regard to admissibility. Those who advocate the general recognition of the technological devices in investigation contend that, the courts do not indulge in creative inquiries when applying law to new technologies and technological changes. They complain that the courts seem to be inclined applying the same old property-based principles in the cases at hand. Whereas the opponents of this philosophy seem all praise to the privacy rights of individuals, all fingers pointed to the landmark case of K. S. Puttaswamy v. Union of India, 2017 which has accredited privacy to the status of fundamental right. Thus as a solution to this issue, it is not a revolution what is needed, but a reform at par with time which could bring physical intrusion to date. (William J. Hoese, 1964).

6. Conclusion with Suggestions and Recommendations

The present paper highlights the mammoth pace at which we are moving ahead with technology lately. And it would rather be noticed that as and when the offenders reach out to technology for pursuing their evil intent, the legal systems of the world also keep at par with them by availing the same eventually ending up in the invasion of its citizens' privacy. The present paper reveals the vast leap made in the area of technology and its wise incorporation into the field of evidence-collection techniques by the law enforcement agency lately. This leads us to the issue: Are the States to put at risk the core human rights viz., the privacy and liberty of its population for the sake of apprehending a few deviants?

The authors herein has examined how technology has remoulded, reframed and reshaped the crime commissions; and how the law enforcement agencies have attempted to be at par with it by adoption of latest techniques for identification, data aggregation, and collection technologies; and how all of these virtually intersect with security and privacy interests of the individuals (K. A. Taipale, 2005). The paper thenceforth highlighted the renowned argument that holds privacy and security at opposite poles. The authors in fact are of the opinion that there is an imminent requirement for a balancing act holding privacy and security in its two pans which happens to be a wicked problem for the adjudicators if not for the legislators. And it is evident that attaining and preserving a proper equilibrium among the values of surveillance, disclosure and privacy is a delicate and difficultprocedure in all jurisdictions. It is particularly true in the society which seeks liberty and stability on one hand and scientific development on the other (Alan F. Westin, 1966). Meeting the challenge to privacy in this era of information outburst requires evolution or moulding of a law and its doctrines according to the changing circumstances (Ricardo J. Bascuas, 2013).

At this point the author keeping in mind the difficulty of the Indian judge in finding a solution to this problem suggests for a legislative input. Although there is ample scope for judicial discretion, the cases discussed hereinbefore infers inconsistency and unpredictability when dealing with the issue. The discretion available to the Indian Judges to exclude such improperly, unfairly or technologically obtained evidence is presently uncodified, which necessarily leaves a huge vacuum within which they should decide on its' admissibility. The decisions made upon the matter, as is clear has depended on the value choices the Judges imbibe, which obviously differs according to their individual temperaments.

If there is a legislative addition to the existing evidence law pertaining to admissibility of evidence obtained technologically lion's share of the problem is solved. Such a law which clearly states the instances and grounds where the evidence could be admitted and where not; a law which is not

archaic and strictly conventional confusing the judge about the application of law to the cases at hand; a law which is attune with the moving times; a law which enables the judge exercise judicial discretion in a structured manner and evaluating the probative value of the evidence under consideration is the need of the hour.

In this respect, the probable solution would be to enact a statute mostly in the lines of the Police and Criminal Evidence Act, 1984 of Englandwhich would not only ensure the Courts to check the probative value of evidence, but also guarantees police reform in a larger perspective.

Section 78 of the Police and Criminal Evidence Act, 1984 is such a piece of law enabling the judges weigh the evidence obtained appropriately. On close analysis of the provision titled 'exclusion of unfair evidence', one would find that it allows the Court to refuse allowing evidence which the prosecution wish to rely on,on certain prescribed circumstances. The section holds that the Judge should decide on it "having regard to all the circumstances, including the circumstances in which the evidence was obtained..."; and that use of the evidence "would have such an adverse effect on the fairness of the proceedings....", that such exclusion is justified. Thus it is evident that through this provision the system has affirmed and held high the common law discretion, but upon certain specified standards or parameters established by a well-formulated enactment itself.

As a matter of fact the 94th Law Commission of India had submitted its report on similar lines. The authors strongly recommend addition of this provision in the Evidence law. The Commission under the Chairmanship of Justice K.K. Mathew had discussed the scope and ambit of admissibility of evidence back then in 1983 (94th Law Commission Report, 1983). It proposed a change in the strict admission of evidence simply based on relevancy. The Commission observed that such an admission would infer approval of an illegal process of justice (Ayush Verma, 2021). The Report had therein proposed the addition of a provision: Section 166A to the Indian Evidence Act. The proposed provision had provided with the Courts a legislative discretion to be availed if there occurs disrepute in justice administration. They were categorised under the broad heads of: the manner of obtaining evidence; the nature of violations of social values and human dignity; the significance of the evidence and the gravity of the offence; harm caused to the accused and instances like urgency justifying the actions etc.

The authors would also suggest some other criteria in addition to the above-mentioned which would help in ascertaining and weighing the competing interests of privacy and security. It is true that there are genuine and powerful social interests regarding the claims of disclosure and surveillance, but at the same time for the claims of privacy. If privacy is to receive its proper weight in the balancing of such competing values, there is a requirement of a well thought-out, logical and reasoned balancing process with distinct criteria by which authorities could evaluate and appraise claims for surveillance or disclosure by means of the most up-to-date devices. Thus there clearly ought to be a checklist in order to appropriately ascertain its actual probative value which are: what is the actual want for conductingsuch a virtual surveillance?Are there any other substitute methods available other than these technically intrusive procedure? What is the degree of dependabilityof the surveillance-instrument?Whether any actual or impliedconsent to the surveillance has been provided? etc.(Alan F. Westin, 1966).

Detailing the parameters, the authors find it necessary that the surveillance techniques be used by the authorities taking into account the problem of legitimate social importance. The only, but the major requirement being that it must be authorised. That is it be legal and intra vires i.e. a proper procedure for licensing ought to be culled out sound enough so as to intervene the privacy of the individuals. Put in other words the requirement must be grave enough to defeat the risk of jeopardizing the people's freedom and their reasonable and legitimate expectations of privacy. The author surge here that whether to authorize the use of surveillance devices or processes, depends on the specific legal system. But in doing so the respective state must regulate the surveillance; i.e., the 'who, when, and how' should be well clarified. First, rules must be set out as to limiting who may carry out such surveillance. Second, detailed regulations should be set for the scope, duration, and operation of the surveillance. Third, some general agency ought to be created to set the standards for surveillance, supervise practices under the rules, investigate compliance, and hear complaints about misconduct. The fourth step is to formulate rules governing the use of such information so obtained. In courts the use ought to be strictly limited to information gathered in full conformity with the control system. The authors consider refusal to allow evidence collected in violation of the control system would be the simplest and most practical way of building respect for the rules.

Another suggestion put forth by the authors is that the law enforcing agencies before opting in and proceeding with the particular scientific device for collecting the evidence is to analyse and check whether there exists any other alternative method which are less violative of individual and organizational privacy as against the proposed newer surveillance devices and techniques. Here, the burden of proof should be on those seeking authorization for such surveillance to establish that other techniques are not available.

Yet another recommendation is the requirement of consent. It is to be checked in each of thecontexts of surveillance. The use of consent mustbe for the information obtained by means of surveillance. Neither law nor public pressure whatsoever ought to force anyone to surrender his privacy. Here the person giving up privacy should be an adult of sound mind and he does that for psychological, commercial, or humanitarian reasons. The authors here point out that privacy is not said to be violated when a person submits to a psychological test for counselling or medical purposes or as a means of perfecting the test, takes experimental drugs, or gives personal data to a private or governmental survey.

Appendix

- Access-control system→The system allows the entry into areas and tracks employee movements. It records the time and date of entry and also the user-information. It includes basically the fingerprint scanners, retinal scanners, voice recognition systems, and other such identification mechanisms. Investigators may use these to prove the absence or presence of a person at a specific location; scrutinize profiles or patterns of activity which might be evil-intended. Investigators make use of these to procure telephonic call content which gets recorded, the time stamp and date of the messages etc. The callers could also be identified by the content of the incoming messages or even establish the undercover identities.

- Internet service provider→Acompany provides persons and companies access to Internet and other similar services like virtual hosting and website building. It can provide the investigation agency following: The subscriber information; the transactional data viz., connection log, location, time, the duration of connection to the internet etc.; and also the content of communications etc. again which would lead the investigation agency to the real criminal. The source of information obtained by the internet is considered to be the accurate. It has the capability of identifying the domain names, the IP addresses, which happens to be an integral part of conducting internet investigations. In fact the types of data available to the investigators through Internet are numerous.

- Black box or Navigation Systems →These can capture information about the vehicle's status, location etc. It will provide all the relevant data for the investigating agency like the operational history of a vehicle which could be used to locate the actual position of a vehicle; to find out the speed and accident reconstruction; to examine conversations in a vehicle etc. among the others.

- Bugging→Involves a tiny e-device to overhear conversation. This is mostly preferred over wire-tapping because; unlike the latter it is capable of picking up many conversations if strategically planted.

- Caller ID enabled device →It recordsthe phone numbers and the like dataconnected with telephone calls. The datarecorded by these include the name of the user, the time-stamp and date of the user. Date or time information is found to be more accurate than that stored in the device itself as that comes from a service provider. Investigators can use these to determine the date, time, and source of incoming calls (e.g., to establish or contradict an alibi or identify co-conspirators). Investigators use these to obtain information as to the calls made, received, and missed; text messages; e-mails messages; voice mails; electronic serial number (ESN); digital images and video; GPS information to include searches or directions saved; suspect movement through cell tracking information; purchase-information; subscriber-information, etc.

- Camera→Thisdevice is used for recording visual images in the form of photographs and videos. It is nowadays set in open areas to deter illegal conduct and also to monitoring or capturing criminal activity. It can be found these days in airports, public roadways, rail depots, banks, ATMs, etc. These camera systems have got the ability to capture activity inside and outside the area where they are located. The information that can be obtained from these cameras usually helps the investigation agency in the following: to prove the presence of persons; vehicle or license plate information; the witnesses for the offence for support or suspect statements; timeline of events; commission of the crime, etc.

- Electronic communication services →These let individuals to communicate by way of a vast range of applications (e.g., instant messaging (IM), Windows Messenger, etc.). These communications may involve text, audio, video, and file transfers. The interesting point to be noted here is that it has the capability of revealing the following: the possible point of origin

of message transfers, which could eventually lead to the suspect's location; identification of the suspect through a screen name; transactional information related to the Internet connection; direct evidence of the crime (by looking into the contents of communications between suspect and victim available by virtue of the online chat); identifying other information about the suspect through the chat programmes. e-mail may be accredited as the starting point or a key element in many investigations nowadays; it being the electronic equivalent of a letter but including attachments or enclosures. This again provides many investigative leads including in it: the possible point of origin of the crime; identification of the account, which can lead to the suspect; transactional information related to the Internet connection etc. Direct evidence of the crime can also be extracted from an e-mail by virtue of the contents of the mail.

- Electronic Surveillance → It refers to the seeing or overhearing of the subjects with the aid of electronic or electrical devices. The use of this technology dates back to the mid nineteenth century. Since then it has been used by the State fairly well to further the societal interest of booking the offenders. And as the technology gravitates to greater heights, the entire debate centres around the compelling state interest versus the need for safeguards to ensure the provisions of Constitution, or may be the interpretative provisions of the Constitution.

- Global Positioning Systems (GPS)→ Receivers along with GPS satellites, finds the position or location of vehicles, subjects or objects containing the receiver which again help in tracking of subjects. The investigators can better pinpoint the location in prescribing a search warrant, mapping a crime scene, etc.

- Keystroke monitoring tools →Theserecords and monitors the keyboard-activity on a computer. It is useful for the investigators for password retrieval and profiling activity in addition to getting to know with whom they are communicating; what type of data are they creating? etc.

- Pen Register→An e-device positioned on telephone-lines which is used to identify the telephone number of calls made from the suspect's phone. This device is frequently used by the investigation agencies in association with the telephone companies to detect fraud and harassment.

- Personal Digital Assistants(PDAs) →PDAs are computers that are handheld made with the like capabilities as those available on a standard personal computer. It has all the personal information management functions in it along with camera, voice recording system, GPS, e-mail, voice mail, infrared transmission, bluetooth, wireless network, web browsing capability, data storage, etc. Forensic analysis of a subject's PDA reveals information of investigative value such as e-mails and text messages; phone or contact lists; notes and digital voice or video recordings etc.

- Photographic surveillance→Thisrefers to the audio-visual gear to photograph persons.

- Radio transmitter→ is an electronic device which, when connected to an antenna, produces

an electromagnetic signal. They are installed on or in packages, persons, or vehicles, which can then be tracked using the direction- finding receivers. These systems capture the date and time of toll passage.

- Sniffers→This is a device used to capture communication directly from a network. It is equivalent to that of a wiretap. The information includes in it network-packet-data, which gives the destination and source of the communication. It is mostly used lawfully by the communication providers and corporate information-technology-departments for protecting and monitoring their computer networks. To investigators, the data gathered with the help of a network sniffer gives the IP-source of the communication, and a complete record of the communications which might be incriminatory.

- User card→Includes customer reward-cards, credit-cards, driver's licenses, club cards etc. Such cards basically hold information on its embedded chip, magnetic stripe, barcode, hologram, RF device, or other such storage technologies. The information connected with it is found to be either on the card itself or is retained at a database of the firm issuing it. The traceable data include purchase history, customer name, address, telephone number, and biometric data. Investigators use these cards to analyse the transaction records helping them in identifying the subject's location, movement, or other actions; analysing the person's spending habits by his card activity. It also would provide lead showing his spending ahead of his genuine income which might hint the chances of illicit proceeds.

- Wire-tapping→It is a technique that employs the use of an e-equipment for intercepting conversations and interactions of non-consenting parties by a third party.

References

- Alan F. Westin (1966), "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance", Columbia Law Review 66. Also available at http://www.jstor.org/stable/1120983.

- Ashwini Vaidialingam (2015), "Authenticating Electronic Evidence: Sec. 65B, Indian Evidence Act, 1872," NUJS Law Review 8. Available at https://heinonline.org/HOL/Page?handle=hein.journals/nujslr8&id=&collection=all&div=6.

- Ayush Verma (2021), "Right to Privacy and Admissibility of Illegally Obtained Evidence". Available at https://blog.ipleaders.in/right-privacy-admissibility-illegally-obtained-evidence/.

- Bert-JaapKoops (2009), "Technology and the Crime Society: Rethinking Legal Protection", Law, Innovation & Technology1, Also available at http://ssrn.com/abstract=1367189.

- BartlomiejKrzan (2021), "Admissibility of Evidence and International Criminal Justice", RevistaBrasileira de Direito Processual Penal 7. Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/rbdpp7&div=9&start_page=161&collection=journals&set_as_cursor=0&men_tab=srchresults.

- Bharat Chugh, Taahaa Khan (2020), "Rethinking the 'Fruits of the poisonous tree' doctrine: Should the 'ends' justify the 'means'?", Available at https://www-scconline-com.eu1.proxy.openathens.net/blog/post/2020/06/15/rethinking-the-fruits-of-the-poisonous-tree-doctrine-should-the-ends-justify-the-means/

- DengkeXie (2021), "Rights Intervention in the Obtainment of Digital Data in Evidence in Criminal Case- An Analysis based on Six typical Cases", Journal of Human Rights 20.Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/jrnlhmch20&div=6&start_page=60&collection=journals&set_as_cursor=0&men_tab=srchresults.

- Hanna Kuczynska (2021), "Mechanisms of Elimination of Undesired Evidence from Criminal Trial: A comparative Approach", RevistaBrasileira de Direito Processual Penal 7. Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/rbdpp7&div=6&start_page=43&collection=journals&set_as_cursor=0&men_tab=srchresults.

- Joseph F. Coates (1972), "The Future of Crime in the United States from Now to the Year 2000", Policy Sciences 3. Also available at http://www.jstor.org/stable/4531467.

- Jerzy Skorupka (2021), "The Rule of Admissibility of Evidence in the Criminal Process of Continental Europe", RevistaBrasileira de Direito Processual Penal 7. Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/rbdpp7&div=7&start_page=93&collection=journals&set_as_cursor=0&men_tab=srchresults.

- K. A. Taipale (2005), "Technology, Security And Privacy: The Fear Of Frankenstein, The Mythology Of Privacy And The Lessons Of King Ludd", Yale Journal Of Law and Technology7. Also available at http://digitalcommons.law.yale.edu/yjolt/vol7/iss1/6.

- Khagesh Gautam (2021), "The "Deluded Instrument of His own Conviction:" On the Admissibility of Custodial Statements and Confessions under the Indian Evidence Act, 1872", Indon J. Int'l and Comp. L. 8. Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/indjicl8&div=7&start_page=3&collection=journals&set_as_cursor=0&men_tab=srchresults.

- Law Commission (1983), "Evidence Obtained Illegally or Improperly", 94th Report. Available at "https://lawcommissionofindia.nic.in/51-100/Report94.pdf.

- Lindsay Freeman(2021), "Hacked and Leaked: Legal Issues Arising from the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases", UCLA J. INT'l L. Foreign Affairs25. Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/jilfa25&div=16&start_page=45&collection=journals&set_as_cursor=0&men_tab=srchresults.

- LucynaKirwil (2004), "Changes in the Structure of Crime during the Transition Period in

Poland", International Journal of Sociology 34. Also available at http://www.jstor.org/stable/20628719.

- Morris Ploscowe (1963), "New Approaches to the Control of Organized Crime", ANNALS, AAPSS 347. Available athttp://www.jstor.org/stable/1036555.

- Orin S. Kerr (2004), "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution",Michigan Law Review 102.Available athttp://www.jstor.org/stable/4141982.

- Peter K. Manning (1992), "Information Technologies and the Police",Crime and Justice 15. Available at http://www.jstor.org/stable/1147621.

- Ricardo J. Bascuas (2013), "The Fourth Amendment in The Information Age", Virginia Journal of Criminal Law 1. Available at http://ssrn.com/abstract=2264854.

- Saugata Talukdar, (2019), "Privacy and its Protection in Informative Technological Compass in India", NUJS Law Review 12(2). Available at https://heinonline.org/HOL/Page?public=true&handle=hein.journals/nujslr12&div=14&start_page=287&collection=journals&set_as_cursor=0&men_tab=srchresults.

- Talha Abdul Rahman (2011), "Fruits of the Poisoned Tree: Should illegally obtained evidence be admissible?",PL . Also available at http://www.supremecourtcases.com/index2.php?option=com_content&itemid=99999999&do_pdf=1&id=20972.

- Thomas Fetzer, Christopher S. Yoo (2012), "New Technologies and Constitutional Law", Routledge Handbook of Constitutional Law. Available at http://ssrn.com/abstract=2360687.

- Thomas K. Clancy (2005), "The Fourth Amendment Aspects Of Computer Searches And Seizures: A Perspective And A Primer", Mississippi Law Journal 75. Available at http://ssrn.com/abstract=1602052.

- TejasKaria, AkhilAnand, BahaarDhawan (2015), "The Supreme Court of India Re-Defines Admissibility of Electronic Evidence in India", Digital Evidence and Electronic Signature Law Review 12. Available at https://heinonline.org/HOL/Page?handle=hein.journals/digiteeslr12&id=&collection=all&div=8.

- Veena Nair (2018), "Review of the Evidentiary Value of DNA Evidence," Nirma University Law Journal 7. Available athttps://heinonline.org/HOL/Page?handle=hein.journals/nulj7&id=&collection=all&div=8.

- Willie J. Elder Jr., "Electronic Surveillance: Unlawful Invasion of Privacy or Justifiable Law

Enforcement". Available at www.yale.edu/ynhti/curriculum/units/1983/4/83.04.07.x.html.

- William J. Hoese (1964), "Electronic Eavesdropping: A New Approach", California Law Review 52. Also available at http://www.jstor.org/stable/3479003.
- William van Caenegem (2007), "New trends in illegal evidence in criminal procedure: general report- common law", Law Faculty Publications. Available athttp://epublications.bond.edu.au/law_pubs.
- Abdul Kareem Telgi v. The State of Karnataka (2017), Available at https://indiankanoon.org/doc/149876113/.(Stamp paper scam case).
- Anvar P.K. v. V P.K. Basheer and Ors. (2014) 10 SCC 473.
- Berger v. New York, 388 U.S. 41 at p. 49 (1967).
- Chinta Devi andors.v. The State (1997), available athttp://www.indiankanoon.org/doc/585998/.
- DharambirKhattar v. Union of India 2013 CriLJ 2011.
- Inspector of Police &Ors. v. N.M.T. Joy Immaculate, 5 S.C.C. 729 (2004).
- John OhumaOgmekwe and Another v. Intelligence Officer Narcotic (1998), available at http://www.indiankanoon.org/doc/1675487/.
- K. S. Puttaswamy v. Union of India, A.I.R. 2017 S.C. 4161.(Aadhaar Case)
- Khet Singh v. Union of India (2002) available at http://www.indiankanoon.org/doc/853200/.
- MagrajPatodiav. R.K. Birla, S.C. 1295 A.I.R. (1971).
- N. Sri Rama Reddy v. V.V.Giri, (1970) 2 S.C.C. 340.
- Narendra G. Goel v. State of Maharashtra, (2009) 6 SCC).
- State (N.C.T. of Delhi) v. Navjot Sandhu (2005) 11 SCC 600.
- Olmstead v. United States, 277 U.S. 438 at p. 464 (1928).
- Osborn v. United States, 385 U.S. 323 at pp. 342–43 (1966).
- People's Union for Civil Liberties v. Union of India, A.I.R. 1997 SC 568.

- R. M. Malkaniv. State of Maharashtra,A.I.R. (1973) S.C. 157.
- R v. Maqsud Ali, [1966] 1 Q.B. 688.
- Rajesh Talwar v. CBI, (2014) 1 SCC 628 (Arushi-Hemraj twin murder case).
- Ratan Tata v. Union of India, Writ Petition (Civil) Nos. 398 of 2010. Available athttps://vlex.in/vid/ratan-n-tata-vs-546065538.
- S.N. Vijaywargiya v. Central Bureau of Investigation (2017). Available at https://indiankanoon.org/doc/33363690/. (Vyapam Scam case).
- S. Pratap Singh v. State of Punjab, A.I.R. 1964 S.C. 72.
- SajidbegAsifbeg Mirza v. State of Gujarat, Available at http://indiankanoon.org/doc/70789/.
- Selvi v. State of Karnataka, A.I.R. 2010 S.C. 1974.
- Smt. KokiaMahato andOrs. v. The State (1997) available at http://www.indiankanoon.org/doc/359806/.
- State of Himachal Pradesh v. Shri Pirthi Chand andAnotherS.C. 977 A.I.R. (1996).
- Sule Kareem v.Asstt. Collector of Customs, 1998 Cri. L.J. 3052.
- Surendra Koli v. State of U.P., (2011) 4 SCC 80 (Nithari Serial Killings case).
- United States v. Miller, 425 U.S. 435, 443 (1976).
- Vineet Kumar v. CBI, 2019. Available at https://indiankanoon.org/doc/107953018/
- Warden v. Hayden, 387 U.S. 294, 302 (1967).
- Yusufalli Esmail Nagree v. State of Maharashtra A.I.R. 1968 S.C. 147.