A Gateway to all Post Graduate Courses

An MHRD Project under its National Mission on Education through ICT (NME-ICT)

Subject: **Law**

Production of Courseware

- Content for Post Graduate Courses

Paper : **Information and Communication Technology**

Module : **Search, seizure and investigation**

Role	Name	Affiliation
Principal Investigator	Prof. (Dr.) Ranbir Singh	Vice Chancellor, National Law University, Delhi
Co-Principal Investigator	Prof. (Dr.) G.S. Bajpai	Registrar, National Law University Delhi
Paper Coordinator	Dr. Aparajita Bhatt	Assistant Professor, National Law University Delhi
Content Writer/Author	Ms. Mrunal Dattatraya Buva	Visiting Faculty, Indian Law Institute, New Delhi
Content Reviewer	Prof. S.K. Verma	Prof. S. K. Verma (Ex-Dean), Faculty of Law, Delhi University, Former Director, Indian Law Institute, New Delhi

Items	Description of Module
Subject Name	Law
Paper Name	Information and Communication Technology
Module Name/Title	Search, Seizure and Investigations
Module Id	XI
Objectives	To understand the: • Concept of search , seizure and investigation of digital evidence • Safety measures to be taken at the spot of search, seizure and investigation • Stages for the search, seizure and Investigation • American law and its relevance concerning unreasonable search, seizure and investigation • Indian law relating to search, seizure and investigation • Regional/ International guidelines relating to search and seizure and investigation
Prerequisites	The Code of Criminal Procedure, 1973, Art. 21 of Indian Constitution, Principles relating to collection

	of digital evidence in Cyber Forensic Processes, General idea of the European Convention on Cyber Crime, 2001.
Key words	Search and seizure, investigation, digital evidence, confiscation, privacy and search and seizure, provisions relating to search and seizure provided in Code of Criminal Procedure, 1973.

1. Introduction:

The progress of ICT has transformed the manner in which people do day-today trades and interrelate with the world. These connections and communications are recognised and stored on a regular basis accessible by the people and the business firms over and done with the facility was used.

Illustratively, the universal smart phone, overhead and more than a communication device, is an instrument which can preserve a whole note of the communications records, pictures, videos and papers, and a gathering of other severely special contents, such as application records which comprises of place tracing, or commercial records of the consumer. As computers and telephones progressively sanction us to possess massive amounts of peculiar material available at the touch of a switch or display (a standard smart phone can hold anything between 500 MB to 64 GB of data), the growing dependence on PCs as information-silos also exponentially grows the troubles related with the damage of regulate over such instruments and the data they cover. This susceptibility is particularly instinctual in the background of law implementation and the usage of forced national control to uphold safety, contrasted with the person's right to protect their confidentiality.

The right to conduct a search and seizure of persons or places is an essential part of investigation and the criminal justice system. The societal interest in maintaining security is an overwhelming consideration which gives the state a restricted mandate to do all things necessary to keep law and order, which includes acquiring all possible information for investigation of criminal activities, a restriction which is based on recognizing the perils of state-endorsed coercion and its implication on individual liberty. Digitally stored information, which is increasingly becoming a major site of investigative information, is thus essential in modern day investigation techniques. Further, specific crimes which have emerged out of the changing scenario, namely, crimes related to the internet, require investigation almost exclusively at the level of digital evidence.

There are various issues before the court as well as investigating authorities which are needed to be answered, such as:under what circumstances it is reasonable to conduct a search of computers and/or computer files off-site, as op- posed to on-site? Is copying data contained on a hard drive or in some other electronic storage media search or a seizure? Hence in order to find answers to these issues this module highlights the role of courts, investigating authorities and policy makers at national and international level to balance the state's mandate to procure information with the citizens'/ netizens right to protect it.

2. Search , Seizure and investigation Of Digital Evidence[1]

In the conservative surroundings, substances are put in storage in a physical form that can be put in storage materially like data printed on paper, bills, receipts, report, manuscript, etc. which are vulnerable to harm by corporeal approaches such as stealing, robbery, etc., however in the technology era of micro electronic environs, record is put in storage in an incorporealarrangementcreation it a cyberneticspherewherever these restrictions of conservativeprocedures no longer spread on. It also has no corporealborders. Therefore, lawbreakerspursuingdataput in storage in systemPCs with dial-in-access canhave right of entryto that data from almostwherever in the world. The amount of data that can be lifted or the quantity of harm that can be producedby maliciousssoftware developmentencryption may be restricted only by the rapidity of the network and the offender'sapparatus.

2.1 Pre- Planning for Search

When the Investigating Officer is essentiallydo quest in a place anywhere it is allegedthat computer networks or any additional electronic memory devices are likely to be found, it is prudent to call computer forensic expert toalong with the examination group. If, it is not probable, data may be put togetherabout the category, kind, model, operating system, webstructural design, category and place of recordsstoring, distantentréerisks etc., which can be handed on to Forensic Experts for instance that would aidcreatingessentialgroundwork to gather and reserveproof. It must be taken into the consideration that some circumstances, it might not be likely to eliminatethe systemtangibly and recordsmight have to be derivative at the place ofoffense or scene ofexamination. The Investigator or expert needsto possess requiredmass media, software, and other specificobjectsso also exceptional packing things which can precludeharm of records asinformation of magnetic media can be damaged by dirt, lurches and electrostatic surroundings.

3. Safety Measures at the Exploration Spot[2]

3.1 Taking control of the Location

It is verysignificant to safeguard that doubtful or asuspect is not permissible to trace any portion of the PC or additionallydevoted to it whichever by corporealways orby means of wireless device. Meanwhile these days, systems could be associatedover and done withcorporealsystems such as fibre optic, cables, telephones or on Wi-Fi or Wi-max wireless networks or even by the means of a cell phone consuming a wireless message port, the Investigator has to be awfully aware and may find control from an expert, if not accessible on place, on cell phone and proceeds stages as per advices. The Investigator needs to think of that even by using a switch or by providing a direction by the means of a wireless mouse or keyboard or even by giving a direction using an e-mail message, the whole records either could be smeared out or despoiled, doing it unusable for the Investigator. This is also appropriate in the situation of minor instruments or detachable storing devices, which have the dimensions of stowingenormousquantity of records. Therefore, it is very significant that persons existent at the place of the examination are parted from their PCs and all devices are reserved out of their influence. As it is not difficult to damage or abolish cyber evidence, and same can be completed from corner to corner a web, which could be corporeal, or wireless the Investigator must precede all stages to protect the information.

As previously cited, the data in a web link a geenvirons necessityshould not beput in storage at the same site. The information could be present in at a far-off location even in anunlikestate. Hence, it could be significant to discover the stowingposition and take astrokeso. For aninstance, stowage of information is doubted to be placed outside the state; it might be requiredto be aware the Interpol and procee s indispensible follow up stages to question letters rogatory as per the law provided under the provisions Section 166 A Cr PC.

---

[1] Available at http://cbi.nic.in/aboutus/manuals/Chapter_18.pdf accessed 01.05.2014 at 20.00 AM.
[2] *ibid*

Previously,directing the exploration, the Investigator will essentially to choose, if tograbinformation on site, or take hold of hardware for analysis at a CFSL. Whereason fieldinformationconfiscation has the benefit, that one does not have to carry much hardware; one may requirefacilities of a Computer Forensic Expert to download information forexamination and reserverecords for giving it in the Court. When in uncertainty, make use of a Computer Forensics Specialist at the scene, if imaginable, to regulateif one desires to confiscateinformation orconfiscate hardware. In case, anexpert is not accessible, it is endorsed that one confiscates the whole thing.

3.2 Networked Computers

One should not cut offsever connectionsfrom the computer if web linkageor processors are involved, pulling a computer from a network may loss the network, and creates damage to the firm'sactions. It is usually not applied to confiscate acomputer as it needsdetaching all the computers which are connected to it. Hardware confiscation with PCs on a network can be actualcomplex, and one should certainly enlist the help of a Computer Forensics Expert in these cases.

3.3 Planning for the Search

The Examiner or Investigator should follow the following items with him that will facilitate the search: ─

(1) Disks or Cartridges ─ these can be used to stockduplicates of files from the PC for use in his investigation.

(2) Labels ─ to label cables, where they plug in, disks, the various parts of the computer and to write/protect disks.

(3) Screwdrivers and other tools used to dismantle the hardware for seizure.

(4) Gloves ─ remember that often, latent prints can be taken from disks or other storage media or hardware.

(5) Packing materials – rubber bands, tape, boxes, bubble wrap, and if he does not have access to anti-static wrap, paper bags should be used, because they have less static charge than plastic bags.

(6) Camera equipment – to videotape and photograph the scene.

(7) Chain of custody report sheets and other paper to inventories seized evidence. [3]

4 Stages forthe Search and Seizure and Investigation[4]

4.1 Rely on Technical Experts

One should be cautious not to reasonharmthroughout a search as automaticallystowed data can be simplymisplaced. The services of the Computer Forensic Expertshall betaken,everyplaceprobable. The specialists can not only assistthroughout anexamination, but could also contribute in interrogating the firm's technical personnel because they will know what interrogations to question to bring about relevant information for the investigation.

Once, on-site, the Investigator has to assess theapparatus and take preventive steps as referred above. Next, he will need to document the way the system is connected together and take the following steps:

─ (i) Marking&Photo'ing the Arrangement

Marking and photo'ingthe whole thingprevious to disassemblingthe computer is a significantinitial step. Take some general photos of the place of an examination to record its pre-search situation for authorisedresolutions, and to aid as a reference during investigation. Thesepapers on how the

[3] *Supra note 1.*
[4] *Supra note 1*

computer was configured may provide evidencecrucialwhile the PC is re-connected in the Forensic Laboratory. As the IO is capturing the photographs, he musttake close-ups of the front and back of all devices and the manner in which it is joined. He have togive exceptionalconsideration to DIP switches on the backside of certain equipment's that is essential in a specific configuration. These switch settings could inadvertently be moved in the means of transportgeneratingdifficulties for the examiner.

(ii) Label all Parts

The I.O. should mark each portion before he beginsdisassembling any of the devices. He should do labelling to all the connectors and sockets at both tops, and on the system so that re-assembly is not difficult and precise. A good way to do this is to sticky labeleverything its own letter.Illustratively, a power cablemight be marked 'A' on the side and ananalogous label marked 'A' on thesystem portanywhere this plug is to be slot in.

(iii) Power System Down

As per a rule/ regular practice if a computer isshut down, it must not berestarted. Hackers could make their system's delete data if aspecific disk is not in the drive when the system is booted up or if a specific password is not give. Similarly, if the system is on, one mustfind itbefore shutting it down otherwise itcan cancel data. One must recollect a thing that a computer canbe looked like it is turned off however in fact; it can be in a sleep mode. Hackers can fix their computer toeliminate data if not properlystart up from a sleepmode, therefore one may be essential to take away plug or the battery from a laptop/ computer in these situations. The I.O. may inevitablyto shut down thesystem through the operating system despite of simplyplugging it off." however, he does need to pull the plug, he mustplug it off from the back of the system despite of the wall, meanwhile the system isploughed into a back-up power supply it may start a stoppageprocess that could changerecords.

(iv) Dismantle or disassemble the System

After labelling and shutting down the system. It can be disassembled intodistinctmechanisms for transportation. If a system is at a commercialplace and a portion of a network, appropriateprocess should be trailed to appropriatelyseparate the system from the network.

(v) Seize Documentation

Instruction manual for the system should be confiscated,including itsoutlying devices, and particularly the software and operating system. The experts at a Forensic Laboratory require to bringing up to a manual to regulate the type of hardware and its technicalities. Confiscating other papers at the place like records, passwords, and journals may show very useful. Sticky notes, or other pieces of paper around the system that may have passwords or login ID's written on them, should also be seized from the spot.

4.2 *Handling Evidence & Computer Hardware during investigation*

(i) Safeguarding information or Data

The I.O. must also safeguard disks or cartridges he discovers at the place of search with reference to keepsafe the data. Most compact disks and cartridges have alittle slithering tab that precludesaltering the disk information whenfixedproperly. Inserting a blank disk in the hard drive of r system will retain them from booting up from the hard drive if they are inadvertentlyswitched on.

(ii) Packing for Transportation

Once the I.O. or the expert has disassembled the computer, it is ready to be packed for moving to the Forensic Laboratory. Systems parts being subtle are simply damaged and the hard drives that regularlycollect therecords have subtlemachineries, so they should be controlledprudently. One should

not cover the systemmachineries using Styrofoam because small constituent parts candisruption off and become inside the PCproducing it to failure. Antistatic plastic bubble/wrap is favoured.

(iii) To keep ComputerApparatusesorganised

It is required to keep the constituents of each Computer together. This small structuralstage can protecta lot of periodonce the inspectors are trying to rebuild the system.

(iv) Single Machine and seizing Agent

If one individual handles the confiscation of a system, the same one can validate the proof at a trial. This little concern can sidestepmisperception later.

(v) How to transport and store the System

The system should not be placedin the trunk of a Police vehicle. The system should be protected insuch a fashionwhich wouldlessen vibrations which may jiggle a part unfastened. The I.O. should keep thesystem safely, cool dry place away from any devices that discharge electromagnetic signals.

Investigation of Computer Crime Scene and search and seizure of digital Evidence

(A) **Formulate plan**	**(B)** **Approach and Secure Crime Scene**	**(C)** **Document Crime Scene Layout**	**(D)** **Search for Evidence**	**(E)** **Retrieve Evidence**	**(F)** **Process Evidence**

Image 1: Investigation of Computer Crime Scene and search and seizure of digital Evidence

Source: http://www.symantec.com/connect/articles/field-guide-part-five

5. The Fourth Amendment Protection against Unreasonable Search ,Seizure and investigation in American Law:

The scope of the mandate as mentioned in the introduction part of this module is presently being deliberated before the Supreme Court of the United States, which started hearingsubmissions in the cases Riley v. California,[5]and United States v Wurie,[6]on the 29th of April, 2014. The point for the consideration was, if theinvestigating officers should be permitted to pursue the mobile phones of persons,upon lawful detention, without gaining a precise warrant for such search. The casesrelate the events where the accused was in detentionbecause of a minor breach and a search without waslead, which comprised the search of cell phones in their custody. The information exposed in the phones eventuallymanaged to the evidence of added crimes and the sentence of the accused of seriousoffences. The appeal is to surpass the evidence so acquired, on the basis that the search

[5]http://www.supremecourt.gov/oral_arguments/argument_transcripts/13-212_86qd.pdf accessed on. 02.10.2014 at 9.30 PM .

[6]In Wurie, the motion to supress was allowed, while in Riley it was denied. Also see US v Jacob Finley, US v Abel Flores-Lopez where the motion to suppress was denied.

disrupts. Even though, there have been anoverabundance of inconsistentchoices by numeroussubordinate courts (including the judgements in *Wurie* and *Riley*),[7] the Federal Supreme Court for the first time determines the question whether mobile phone searches should need a greateronus under the Fourth Amendment in US Constitution.

The fundamental difficulties arereflections of individual privacy and the right to restrict the state's intervention in privacy issues. The fourth amendment in the Constitution of the United States specificallyprovides safeguard against unwarranted searches and confiscation,[8]nonetheless, discretion has been given to the courts to appreciate situations in which the right to non- intervention would go betterto the interests of attaining information in every case in absence of the precise definition of the term "Unreasonable", leading to comprehensive anddiverse jurisprudence on the matter. The jurisprudence originates from the extensive fourth amendment safeguard against unreasoned government intrusion, where the law is usually that any 'search without warrant is unreasonable,exceptenclosed by sureexclusions. The basis for the safeguard under the Fourth Amendment has an individual standard, which is decided on as per subjective psychological consideration, than that of any objective consideration such as physical location; and encompasses to all conditions where people have a *rational expectation of privacy*, i.e., circumstances where people can reasonablybelieveto have privacy, which is a subjective criterion , and not absolutely reliant on the tangible location of search.[9]

Therefore, the condition of reasonableness is generally only satisfiedonce a search is accompaniedfollowing to issuance of a warrant from an *unbiasedjudge*, by proving *crediblereason* to be certain ofthe evidence of any illegalaction would be based upon such search. Hence, a warrant is a significantrestriction on the search authorities of the investigating officers. Additionally, the safeguardexcludes roving or overall searches and needs *accuracy* of the articles to be searched. The limitationoriginates its authority from the exception rule, which creates a bar to the evidence acquired through unwarranted search or confiscation, foundstraightaway or through added warrants founded upon such evidence, from being used in succeeding prosecutions. Though, there have developednumerousexclusions to the general rule, which inculcates cases where the search proceeds on the legitimatedetention of an accused, a process which is justified by the prospect of unseen weapons upon the accused or of damage caused to the key evidence[10].

If, the appealsucceeds, it would give an exclusion to the law that any search on legitimatedetention arrest is always rational, by making a caveat for the search of electronic devices like smartphones, PDA`s etc. If the court does so, it could be avitalacknowledgment of the point that developing technologies have transformed the notion of privacy outside physical space, and legal rules and principleswhich applied to privacy even twenty years ago, are now out-dated in an era wherepeople cancapture theirperfectlife on an iPhone.

Finding anindividualthese days would not only amount to the recovery of calling cards or cigarettes, but cell phones and systems which can be thevirtual record of an individual's life, somewhatthat could not have been anticipated when the rules were drafted. Mobile phone and computer hunts are the alike of searches of corrodes ofrecords,pictures and individual records, and the bated breath of privacy in these cases is greater than in usual searches. Courts have previouslyconsidered that cell phones and laptops are items in which the operator may have a rationalbelief of privacy by assembling

[7] The Fourth Amendment to the Constitution of the United States of America: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[8] Katz v United States, 389 U.S. 347, 352 (1967).

[9] Stephen Saltzer, American Criminal Procedure

[10] United States v Chan, 830 F. Supp. 531,534 (N.D. Cal. 1993).

themcorresponding to a "padlockedflask" which the law enforcement agency cannot explore and thereforeimpending under the safeguard of the Fourth Amendment.[11]

However, the other side provides, mobile phones and computers alsoclutch data that can be helpful in examining criminal action, and with tools like secludedsmears of accessible computer records,this kind of record iscontinuouslyin the danger of damage if investigation happens late. On the basis of theverbalopinions, being received now, it appears that the Court is beingfiguring out anexactstandardappropriate to novel technologies. The Court is expected to bring togetherdelicaciesprecise to the technology involved – Illustratively, it mightsearching foremergingvariable standards for smartphones and the more basic kind of cell-phones , or it may identify that merelyspecific kinds of evidence may be read,[12]or may advance a rule that would agree to seizure, howevernot a search, of the mobile phone before a search warrant can be acquired.[13] Identifying that transformational technology wants to be replicated in technology-specific legal values is a significant step in preserving a harmonization between law and technology and the addedacknowledgment of a greatervergeaccepted for digital evidence and privacy would go a long way in safeguarding digital privacy in the future. Hence, this fourth amendment has manifested many implications on the other legal disciplines of the world as well

6. Search and Seizureand Investigation Law in India

Indian jurisprudence of search, seizure and investigation and implications on privacy is a completedeparture from that in the USA. Nevertheless it is hard to stringentlysort the severalaspects of the right to privacy; there is no direct or impliedreference of such a right in the Indian Constitution. Even ifjudiciary has also acknowledged the significance of practicalprotections in guarding against perverse governmental intrusion, the appreciation of the inherent right to privacy as an independent right, which may be diverse from the contributory rights which criminal procedure pursues to safeguard (such as abuse of police authority), is deeplymissing. The general law has provided that for the country'sauthority of search and confiscation of evidence is provided in the Code of Criminal Procedure, 1973.

Section 93 offers for the overallpractice of search. Section 93 provides for a magistrate to issue a warrant for the search of any "document or thing", including a warrant for general search of an area, where it trusts it is required for the purpose of investigation[14]. The meticulousness of the search warrant is not a condition under S. 93(2);therefore a warrant might be for common or roaming search of a place. Section 100[15], which additionally states that for the search of a closed place, includes certain protections such as the attendance of witnesses and the prerequisite of a warrant before a police officer may be permittedaccess into the closed place. However, under S. 165 and S. 51 of the code[16], the necessities of a search warrant are discharged. S. 165 bestows the warrant prerequisite and offers for an officer in charge of a police station, or any other officer duly approved by him, to execute the search of any location as long as he has reasonablebasis totrust that such search would be for the perseverance of an investigation and a confidence that a search warrant cannot be acquiredwithout undue delay. Additionally, the officer leading such search must *as far as possible* write down the details for such certainty in writing prior to undertake the search. Section

[11]The decision in *Smallwood* v. *Florida* No. SC11-1130, before the Florida Supreme Court, made such a distinction.
[12]*State Of Maharashtra* v. *NatwarlalDamodardasSoni*, AIR 1980 SC 593; *Radhakrishnan* v. *State of UP*, 1963 Supp. 1 S.C.R. 408
[13]*M.P. Sharma* v *Satish Chandra*, AIR 1954 SC 300
[14] Sec. 93 of Code of Criminal Procedure, 1973
[15] Sec. 100 of Code of Criminal Procedure, 1973
[16]Sec. 165 and S. 51 of Code Criminal Procedure, 1973

51[17]provides that another express exception to the condition of search warrants, by permitting the search of anindividualdetainedlegally provided that the detainedindividual might not might begranted a bail, and needs any such confiscated items to be in black and white in a search memo. As long as these circumstances are satisfied, the investigating authority has absolutecontrol to search anindividual upon detention. Where the detainee can be granted a bail as per the warrantor, in cases of arrest without warrant, as per the legislation the search and confiscation of such person may not be regular, and the evidence sogathered would be conditioned tomore scrutiny by the court. However, despite ofnominalsafeguards, there is no added procedural safeguard of individual privacy, and the authorities of search of the investigating officers aretremendouslycomprehensive and unrestricted. Actually, there is a lack of the exception rule as a safeguard as well, it shows that, unlike under the Fourth Amendment under US law, the non-compliance with the practical conditions of search would not by itself make the proceedings infructuous or defeat the evidence so established, but would only subject to an irregularity which must be justextraaspectaccepted inassessing the evidence[18].

The extent of the imputation of the Fourth Amendment protection as given in USA against irrational governmental meddling in the Indian constitution is also indeterminate. A direct charge of the Fourth Amendment in USA into the Indian Constitution has been ignored by theHon`ble Supreme Court of India.[19]Nonetheless the allusions to the Fourth Amendment have typically been appealed on truths where irrationalinterruptions into the homes of persons were face up to, the indirect charge of the right to privacy into the right under Article 21 of the Constitution[20], appealing the right to privacy as a right to non-interference and a right to live with dignity, provides that the reflectionsof the right to privacy under the Constitution are not just objective, or corporeal, but be subject to the individual facts and circumstances, i.e. its effect on the right to live with dignity[21].Additionally, the court has explicitly struck down provisions for search and seizure which provides an over extensive and unrestricted authorities on the executive in absence of law courtexamination, considering that searches must be conditioned to the principle of proportionality, and that a provisionpossible cause to effect any search.[22]The Fourth Amendment protection in USA against unreasonable intervention in personal matters by the state is a beneficial standard to assess privacy, since it attributes a concept of privacy as an inherent right as well as acontributory one, i.e. privacy as non-interference is a good in itself, despiteof the rights it helps to achieve, e.g. the freedom of movement or speech.

In the matter of *State of Punjab* v *Amritsar Beverages Ltd*[23]**,** it was held that the proper course of action for officers in such circumstances was to make copies of the hard disk or obtain a hard copy, affix their signatures or official seal on the hard copy and furnish a copy to the dealer or person concerned." However, concerning digital privacy in precise, Indian law and policy has become unsuccessful tomeet thetests that new-fangled ICT pose to privacy and has in fact been reverting, by involving in surveillance of online transactions and by permitting governmental right to usethe online information like emails, website logs, etc. without judicial check.[24]In the era of ICT and of privacy being located at more risk, laws which were once considered rational now, have become absolutely insufficient in ensuring freedom and liberty as provided by the right to privacy. The discrepancy is even more noticeable in cases of investigation of cyber-crimes which depend on almost entirely on electronic evidence, such as those essentiallyprovided under the Information Technology Act, 2000

[17] Sec. 51 of Code of Criminal Procedure, 1973

[18]*State Of Maharashtra* v. *NatwarlalDamodardasSoni*, AIR 1980 SC 593; *Radhakrishnan* v *State of UP*, 1963 Supp. 1 S.C.R. 408

[19]*M.P. Sharma* v *Satish Chandra*, AIR 1954 SC 300

[20]*Kharak Singh* v *State of UP*, (1964) 1 SCR 332; *Gobind* v *State of Madhya Pradesh*, 1975 AIR 1378

[21]*Supra* note 5

[22]*Ibid*

[23] 2006 IndLaw SC 3911

[24]*District Registrar and Collector* v. *Canara Bank*, AIR 2005 SC 186, which related to S.73 of the Andhra Pradesh Stamps Act which allowed 'any person' to enter into 'any premises' for the purpose of conducting a search.

but investigated under the overallprocessprovided in the Code of Criminal Procedure, 1973; as mentioned above.The processes for investigation of cyber-crimes and the search and seizure of electronic evidenceneed special acceptance and must be brought in line with modifying shiftingstandards. Section 80 of the IT Act, 2000 deals with the search and seizure of computer data on connected systems, if there is reasonable justification to do so.[25] It has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of inspector or any authorized officer of central government or state government. Such officer is empowered to arrest without warrant a person found therein who is reasonably suspected of having committed or of committing or being about to commit any offence under this Act. However, this section may be misused easily. Unless it is reasonably suspected that a person has committed, is committing or is about to commit an offence, he should not be arrested without warrant. Otherwise cybercafés, in particular could be adversely affected[26]. Though S.69 and 69B provides law for investigation of certain crimes,[27] it needs search if direction is given by competent authority, i.e. the Secretary to the Department of IT in the Government of India, the authority[28] for search and seizure is also provided in various other rules, such as rule 3(9) of the Information Technology (Due diligence observed by intermediaries guidelines) Rules, 2011[29] which permitsadmission to information from intermediaries by a simple written order by any agency or person who are lawfully authorised for investigative, protective, cyber security or intelligence activity; or under rule 6 of the draft Reasonable Security Practices Rules, 2011[30] framed under Section 43A of the Information Technology Act, where any government agency may, for the prevention, detection, investigation, prosecution, and punishment of offences, obtain any personal data from an intermediate "body corporate" which stores such data. Hence, the rules enclosed for inquiry of electronic evidence, do not encourage much reliance whereprotection privacy is concerned. In the absence of preciseguiding principle or modifications to the search and confiscationprocesses of electronic evidence, the insufficiencies of spread overoldcriterionsamounts to unreasonable interferences of privacy and liberties isanoddness which needssolution by the judges and law makers of the nation.

7. Cyber Crime Convention on Search, Seizure and Investigation[31]

The Convention acclimatisesold-style procedural methods, such as search and seizure, to the noveltechnical environment. Furthermore, new dealings have been shaped, such as acceleratedprotection of data, in order to safeguard that old-styleactions of gathering, such as search and confiscation, stayin effect in the unpredictablecyber world. As info in the novel ICT environment is not always motionless, but may be flowing in the procedure of communication, other old-stylegathering procedures pertinent to ICT, such as instantaneousgathering of traffic data and interception of data information, have also been followed with regard to allow the gathering of digital information which is in the procedure of communication. Some of these methods are given in Council

[25] Section 80 of the Information Technology (Amendment) Act, 2000

[26]Karnika Seth, IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers, National Seminar on Enforcement of Cyberlaw , New Delhi on 8th May 2010 accessed on 0312.2014 at 8.20PM.

[27]S. 69 and 69B of the Information Technology (Amendment) Act, 2000.

[28]Procedures and Safeguards for Monitoring and collecting traffic data or information rules 2009, *available at*http://cis-india.org/internet-governance/resources/it-procedure-and-safeguard-for-monitoring-and-collecting-traffic-data-or-information-rules-2009accessed on. 03.11.2014at22.57 AM..

[29]the Information Technology (Due diligence observed by intermediaries guidelines) Rules, 2011

[30] The Information Technology (Reasonable security practices and Procedures and sensitive personal data or information) Rules, 2011 available at http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf accessed on 03.11.2014at22.57 AM..

[31] Convention on Cybercrime, Budapest, 23.XI.2001 available at http://conventions.coe.int/Treaty/en/Treaties/html/185.htm accessed 08.11.2014 at 20.57 AM.

of Europe Recommendation No. R (95) 13 on difficulties of criminal proceduralcode associated with ICT.[32]

7.1 Investigation

The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.

In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence[33].

7.1.1 Procedural law

The articles in Section 2 describe certain procedural measures to be taken at the national level for the purpose of criminal investigation of the offences established in Section 1, other criminal offences committed by means of a computer system and the collection of evidence in electronic form of a criminal offence. In accordance with Article 39, paragraph 3, nothing in the Convention requires or invites a Party to establish powers or procedures other than those contained in this Convention, nor precludes a Party from doing so[34].The technological revolution, which encompasses the "electronic highway" where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. Equally, safeguards should also be adapted or developed to keep abreast of the new technological environment and new procedural powers[35].

One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation[36].All the provisions referred to in this Section aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings. The drafters of the said Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.[37]

[32] Explanatory Report on Convention on Cybercrime (ETS No. 185)
[33]Id. at pt29.
[34] Pt.131 of *Supra* note 32.
[35] Pt.132 of *Supra* note 32.
[36] Pt.133 of *Supra* note 32.
[37] Pt.135 of *Supra* note 32.

The procedures in general refer to all types of data, including three specific types of computer data (traffic data, content data and subscriber data), which may exist in two forms (stored or in the process of communication). The applicability of a procedure to a particular type or form of electronic data depends on the nature and form of the data and the nature of the procedure, as specifically described in each article[38].All the articles in the Section refer to "competent authorities" and the powers they shall be granted for the purposes of specific criminal investigations or proceedings. In certain countries, only judges have the power to order or authorise the collection or production of evidence, while in other countries prosecutors or other law enforcement officers are entrusted with the same or similar powers. Therefore, 'competent authority' refers to a judicial, administrative or other law enforcement authority that is empowered by domestic law to order, authorise or undertake the execution of procedural measures for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings[39].

The measures described in the articles operate only where computer data already exists and is currently being stored. For many reasons, computer data relevant for criminal investigations may not exist or no longer be stored. For example, accurate data may not have been collected and retained, or if collected was not maintained. Data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings. Sometimes there may be no business reason for the collection and retention of data, such as where customers pay a flat rate for services or the services are free. Article 16 and 17 do not address these problems[40].

7.1.2 Expedited preservation of stored computer data

Articles 16 and 17 refer only to data preservation, and not data retention. They do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. The preservation measures apply to computer data that "has been stored by means of a computer system", which presupposes that the data already exists, has already been collected and is stored. Furthermore, as indicated in Article 14, all of the powers and procedures required to be established in Section 2 of the Convention are ‘for the purpose of specific criminal investigations or proceedings’, which limits the application of the measures to an investigation in a particular case. Additionally, where a Party gives effect to preservation measures by means of an order, this order is in relation to "specified stored computer data in the person’s possession or control" (paragraph 2). The articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings[41]. These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. These directives do not prevent member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specific investigations[42].

7.1.3 Expedited preservation of stored computer data (Article 16)

Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal

[38] Pt.136 of *Supra* note 32.
[39] Pt.138 of *Supra* note 32.
[40] Pt.150 of *Supra* note 32.
[41] Pt.152 of *Supra* note 32.
[42] Pt.154 of *Supra* note 32.

investigation or proceeding[43]. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data[44].

7.1.4 Production order (Article 18)

Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.[45]A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation[46].

In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes[47].

7.2 Search and Seizure

In adjusting theold procedural legislations to the ICT world, the query of suitable terminology ascends in thewordings of this section. The choices inculcated preservingout-dated language ('search' and 'seize'), practising novel and extra technologically concerned withsystem terminology ('access' and

[43] Pt.158 of *Supra* note 32.
[44] Pt.163 of *Supra* note 32.
[45]Pt. 170 of *Supra* note 32.
[46]Pt. 175 of *Supra* note 32.
[47]Pt. 178 of *Supra* note 32.

'copy'), as accepted in writings of other global forum on the issue, or engaging a cooperation of variedterminology ('search or similarly access', and 'seize or similarly secure'). As there isa requirement of reflecting the development of ideas in the cyber world, so also recognise and preserve their old-stylebackgrounds, the elasticmethod of permitting States to practice either the old ideas of "search and confiscation" or the new concepts of "admission and duplicating" is active.[48]

Another protection in the convention is that the authorities and processes shall "integrate the standard of proportionality." Proportionality shall be applied by each Party with reference withapplicableprovisions of its national law. For European countries, this will be resulting from the standards of the 1950's Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its appropriate jurisprudence and national law and jurisprudence, that the control or procedure shall be relative to the nature and conditions of the offence. Other States will be concerned to the provisions related to their law, such as restrictions on over extensiveness of creation orders and rationalitywishes for searches and seizures. Also, aclearrestraint in Article 21 that the responsibilities concern to interception events are in concern t to a variety of serious offences, dogged by national law, is an obviousinstance of the request of the proportionality standard.[49]

The reference to 'order or similarly obtain' is planned to permit the use of other lawfulprocedures of realisingprotection than just by means of a legal or executive order (e.g. from police or prosecutor). In some States, protection orders do not occur in their procedural law, and records can only be well-maintained and acquired through search and seizure or creation order. Flexibility is proposed by the practice of the phrase 'or elseget' to authorise these States to execute thisprovision by the practise of these means. Nonetheless, it is suggested that States cogitate the instituting of authorities and procedures in fact theaddressee of the order to preserve the data, as rapid action by this person can consequence in the more speedyapplication of the protectionevents in specific cases.[50]

The power to order or in the same wayfinds the speedy preservation of identified computer data spread over to any type of PC storage data. This can comprise any type of data that is identified in the order to be well-kept. It can comprise, illustratively, business, health, personal or other records. The measures are to be recognised by Parties for use "in precise where there is a basis to believe that the PC data is particularly susceptible to loss or amendment." This can comprisecircumstances where the data is subject to a short period of retaining, such as where there is a business policy to remove the data after a certain period of time or the data is normallyremoved when the storingstandard is used to record other data. It can also mention to the nature of the custodian of the data or the apprehensive manner in which the data is put in storage. Though, the keeper wasunreliable, it would be more protected to resultprotection by means of search and seizure, rather than by means of an order that could be challenged. A specific orientation to "traffic data" is prepared in paragraph 1 in order to signal the requirementsspecific applicability to this type of data, which if composed and reserved by a service provider, is usually held for only a short period of time. The orientation to "traffic data" also offers a link between the procedures in Article 16 and 17.[51]

Paragraph 2 stipulates that where a member state stretches effect to protection by means of an order, the order to retain is with reference to "identifiedstoragesystem data in the individual'scustody ". Hence, the datastorage in factis in the custody of an individual or it may be put in storage to a different place, however under the custody of this person. An individual who obtains the direction is

[48] Pt. 137 of *Supra* note 32.
[49] Pt.146.of *Supra* note 32
[50] Pt. 160.of*Supra* note 32.
[51] Pt. 161 of *Supra* note 32.

under an obligation toretain andsustain the veracity of the system data for timeduration as long as essential, up to a maximum of 90 days, to allow the competent authorities to pursue its disclosure." The national law of a member state shouldstipulate a maximum period of time for which data, subject to an order, must be preserved, and the order should stipulate the precise timeduration that the specified data is to be preserved. The time duration should be as long as essential, up to a maximum of 90 days, to allow the competent authorities to take added legal measures, such as search and confiscation , or access or securing, or the issuance of a production order, to get the disclosure of the data. A Party may offer for succeeding renewal of the production order. With reference to this, reference should be made to Article 29, which provides a mutual assistance request to get the speedyprotection of data put in storage by the way of a computer system. That article stipulates that retention caused in reply to a mutual assistance request "shall be for a period not less than 60 days in order to permit the requesting Party to submit a request for the search or similar access, confiscation or similar safeguarding, or disclosure of the data."[52]

The provision aims at updating and consistentnational laws on search and confiscation of storage system data for the objective of attaining evidence with reference toexact criminal investigations or proceedings. Any national criminal procedural law inculcates authorities for search and seizure of physicalthings. Nevertheless, in various jurisdictions system storage data per se will not be regarded as a tangible thing and hence cannot be protected on behalf of criminal investigations and proceedings in a parallel method as tangible objects, other than by safeguarding the data medium upon which it is storage data. The object of Article 19 of the said Convention is to create an equal power connecting to data storage.[53]

In the old-style search environment aboutpapers or records, a search includescollecting evidence that has been recorded or registered in the past in tangible form, such as ink on paper. The investigators search or inspect such recorded data, and confiscate or physically take away the physical record. The meeting of data takes place within the period of the search and in respect of data that happens at that time. The prerequisite for gaining legal power to start a search is the presence of grounds to believe, as arranged by local law and human rights protections, which such data be existent in a specificposition and will afford evidence of a precise criminal offence.[54]

With reference to the search for evidence, in precisesystem data, in the new technological environment, numerous of the features of anold-style search remain. Illustratively, the collection of the data happens during the duration of the search and with reference to the data that is existent at that time. The requirements for gaining legal authority to assume a search continue the same. The degree of beliefneeded forgaining legal approval to search is not dissimilar whether the data is in tangible form or in electronic form. Likewise, the trust and the search are with reference of data that previouslysubsists and that will give evidence of anexact offence.[55]

Though, with regard to the search of computer data, added procedural requirements are needed in order to safeguard that computer data can be gained in a way that is equally real as a search and confiscation or seizure of a physical data carrier. There are numerouscauses for this:

First, the data is in incorporeal form, such as in an electromagnetic form.

Second, while the data may be read with the help of computer device, it cannot be confiscated and moved away in the similar sense as can a written record.The corporeal medium on which the incorporeal data is put in astorage (e.g., the computer hard-drive) must be confiscated andmoved away, or a copy of the data must be made in either tangible form,illustratively, print-out of a computer or intangible form, on a tangible form (e.g., diskette), before the tangible medium comprising the copy can be confiscated andmoved out. In the latter two circumstances, where such copies of the data

[52]Pt. 162 of *Supra* note 32.
[53]Pt. 184 of *Supra* note 32.
[54] Pt.185 of *Supra* note 32.
[55] Pt.186 of *Supra* note 32.

are made, a copy of the data remains in the PC or put in storage device. National law should offer a control to do such copies.

Third, due to the connectivity of computer systems, data may not be put in storage in the specific system that is searched, but such data may be freelyavailable to that computer. It could be put in storage in connected data storage equipment that is linkedstraight to the computer, or associated to the system indirectly through ICT, such as the Internet. This might or might not need new laws to allow an allowance of the search to where the data is trulyput in storage , or the use old-style concept of search authorities in a more harmonised and speedymethod at both positions.[56]

Paragraph 1 needs Parties to allow law implementationestablishments to access and search computer data, which is delimited either within a PC or part of it (such as a connected data storage device), or on an independent data storage medium (such as a CD-ROM or diskette). As the definition of "computer system" in article 1 refers to "any device or a group of inter-linked or interrelated devices", paragraph 1 provides the search of a computer system and its connectedmechanisms that can be regarded together as developing one separate computer system (e.g., a PC connected to a printer, other storage devices, a LAN etc.). Occasionally data that is physically put in storage in another system can be lawfully accessed through the searched computer system by forming anassociation with other diverse computer systems. This condition, connectingrelations with other computer systems by the way of ICT networks inside the same territory is discussed in paragraph 2 e.g., Internet.[57]

Though search and seizure of a "computer-data loading medium in which system data may be put in storage" (paragraph 1 (b)) may be assumed by the usage of old-style search powers, time and again the implementation of a system searchneeds both the search of the PC and any linked computer-data storage medium (e.g., diskettes) in the instantarea of the computer system. Because of thisassociation, aninclusive legal expert is discussed in paragraph 1 to include both circumstances.[58]

Article 19 applies to system storage data. With reference to this, the issue arises,if an unopened e-mail in the mailbox of an ISP until the recipient will download it to one`s PC, has to be regarded asPC storage data or as data in transit. As per the law of some member states s, that e-mail is part of a ICT, hence, its data can only be acquired byexerting the power of interception, whereas other legal systems appreciates such message as data storage to which article 19 applies. Hence, member state shouldamend theirlegislations withregard to this question todecide what is suitable within their national legal systems.[59]

The concept of' search or similarly access is also discussed. The use of the old-styleterm 'search'provides theimpression of the implementation of forcedcontrol by the State, and specifies that the authority mentioned in this article is similar to old concept of search. 'Search' connotes the meaningi.e. to pursue, read, scrutinise or evaluation data. It comprises of the ideas of searching for data and examining the data. Whereas theterm 'access' is anunbiasedconcept, however it reproduces precise computer terminology. Both positions are used to harmonise theold and modern idea of the search and access.[60]

[56] Pt.187 of *Supra* note 32.
[57] Pt. 188 of *Supra* note 32.
[58] Pt. 189 of *Supra* note 32.
[59] Pt. 190 of *Supra* note 32.
[60] Pt. 191 of *Supra* note 32.

The orientation to 'in its territory' is anaide memoire that this provision, as all the provisions in this Section, provides only methods that are obligatory to be occupied at the national level.[61]

Paragraph 2 permits the investigating authorities to spread their search or similar admission to additional computer system or part of it.If they have basis tohave confidence in that the data essential is stowed in the otherPC. The other computer system or part of it must, though, also be 'in its territory'.

The Convention does not recommend how an extra time of a search is to be allowed or started. This is subject tonational laws. Illustratively, probablesituations are: authorising the judicial or other power which approved the computer search of a precise computer system, to authorise the allowance of the search or alikeadmission to a linked system if he or she has basis to trust that the connected computer system may comprise the exact data that is being required; authorizing the investigative establishments to spread an official search or similar admission of anexact computer system to a linked computer system where there are alikebasis to consider that the exact data being pursued is put in storage in the other computer system; or working out search or similar admittanceauthorities at both places in a co-ordinated and speedymethod. In all cases the data to be searched must be legally accessible from or available to the initial computer system.

This provision does not discuss ‘Trans border search and seizure', whereby States could search and confiscated data in the territory of other States without having to go through the usual channels of mutual legal help. This concept isdeliberated in the Chapter on international co-operation of the Convention.[62]

Paragraph 3 discourses the subjects of authorizingcapableestablishments to seize or likewise secure computer data that has been searched or similarly accessed under paragraphs 1 or 2. This comprises the control of confiscated of computer hardware and computer-data storing media. In certain cases, for example when data is deposited in unique effective systems such that it cannot be copied, it is necessary that the data transmitter as a whole has to be confiscated. This may also be essential when the data transmitter has to be scrutinised in order to retrieve from it older data which was overwritten but which has, nonetheless, left traces on the data carrier.[63]

In the Convention, to confiscate ' means to move the corporeal medium upon which data or evidence is documented, or to make and preserve a copy of such data or information. ‘Seize’ comprises the use or confiscation of programmes required to admit the data being confiscate. So also using the old-style term 'seize', the term 'similarly secure' is comprisedto manifest other ways by which imperceptible data is destroyed, made unreachable or its switch is then taken over in the computer environment. Since the measures relate to stored incorporeal data, supplementarymethods are obligatory by competent authorities to protect the data; ‘maintain the integrity of the data', or maintain the ‘chain of custody’ of the data,signifying that the information which is copied or removed be stored in the State in which they were bring into being at themoment of the seizure and become untouched during the time of criminal proceedings. The perioddenotes to create control over moving out the data.[64]

The interpreting inaccessible of data can compriseencoding the data or otherwise technologically disagreeing anyone enters to that data. This measure could usefully be practical in circumstances where hazard or societaldestruction is engaged , such as virus programs or directions on how to make viruses or bombs, or where the data or their information t are unlawful, (E.g.:Child Pornography). The word 'removal' is projected to express the idea that while the data is detached or rendered

[61] Pt.192 of *Supra* note 32.
[62] Pt.193 of *Supra* note 32.
[63] Pt.194 of *Supra* note 32.
[64] Pt.195 of *Supra* note 32

inaccessible, it is not removed, but remain in existence. The suspect is provisionallydisadvantaged of the data, but it can be refunded following the consequence of the criminal investigation.[65]

Thus, confiscated or likewise secure data has two tasks:

1) Tocollect evidence, by copying the data, or

2) Toseize data, such as by duplicating theinformation andafterwardsinterpreting the newform of the data inaccessible or by eliminating it. The seizure does not suggest a final removal of the seized data.[66]

Paragraph 4 provides aforced measure to enable the search and seizure of system data. It discourses the appliedissue that it may be problematic to access and recognise the data required as evidence, given the amount of data that can be administered and put in storage, the distribution of safetyprocedures, as well as the nature of computer processes. It identifiesthose system administrators, who have actual knowledge of the computer system, may berequired to be referredwith reference to the technical modalities about how best the search should be accompanied. Therefore, thispermits legal implementation toforce a system manager to help, as it is a practical, responsibility of the search and seizure.

This authority is not only of advantage to the investigating authorities, but without such assistance, enforcement authorities could continue on the searched sites and avoidthe admission to the PC for long phases of time while taking the search. This could be financialload on authentic businesses or consumers and subscribers that are deprived ofentrance to information during this time. A way to order the assistance of well conversantpeople would assist intaking searches more actual and cost effective, both for legal implementation andeffect on innocent persons. Legally binding a system manager to help may also relieve the manager of any prescribed or other responsibilities not to release the data[67].

The data that can be well-organized to be given is that which is essential to allow the responsibility of the discovery andconfiscation, or the likewiseretrieving or safeguarding. The provision of this info, but, is limited to that which is "sensible". In some situations, sensible provision may comprise revealing a password or other safety measure to the police. But, in other situations, this may not be sensible; illustratively, where the revelation of the password or other safetyprocesses wouldperverselyaffect the privacy of other operatorsor information that is not sanctioned to be searched. In such situation, the provision of the "required information" might be the revelation, in a form that is understandable and legible, of the real data that is being sought by the competent authorities[68].

Under paragraph 5 of this article, it is provided that the procedures are subject to circumstances and protections provided for under local law on the basis of Article 15 of this Convention. Such circumstances may comprise provisions connecting to the appointment and monetaryreimbursement of witnesses and experts.[69]

Furthermore the drafters discoursed in the scheme of paragraph 5 if involved parties should be informed of the responsibility of a search procedure. In the cyber world it may be fewerdeceptive that info has been searched and copied than that a confiscated in the cyber world took place, where seized articles will be tangiblylost. Legislations of some member state do not offer for a responsibility to inform in the case of old concept of search. For the Convention to need notification with reference to a system search would produceaninconsistency in the legislations of these Member States. Whereas, some Parties may cogitate notification as an importantpart of the measure, in order to continue the

[65] Pt.196 of *Supra* note 32.
[66] Pt.197 of *Supra* note 32.
[67] Pt. 198 of *Supra* note 32.
[68] Pt. 199 of *Supra* note 32.
[69] Pt. 200 of *Supra* note 32.

difference between system search of storage data (which is usually not intended to be a secret measure) and interception of flowing data (Articles 20 and 21). The matter of notification, therefore, is subject to be dogged by local law. If member states contemplate a system of binding notification relating to individuals, it shall bekept inattention that such notification may create a bias the investigation. If such a dangersubsists, delayin the notification should be taken into the considered[70]

Points to Ponder

Role of the system

- The search warrant should specify the system's role in the crime and reason as to itscontents regarding evidence.

Establishment of Nexus

- Establishment of assumption as to find digital evidence at the search premises should be required to be done.

State evidence required

- The evidence as to the possibility of reason to search for it and any evidence of proprietorship of the computer should be specifically state.

Use of Specific Investigation language

- Investigation language to be adaptedto the specific facts of your case.

Protection of integrity of the investigation

The protection of the integrity of the investigation and informants or to avoid the disclosure of intellectual property should be taken into the consideration.

Conclusion:

The novelchanging aspects of computer searches and seizures teach vital lessons about the Fourth Amendment in USA and Information and technology legislations in India, Regional International law as provided in European Convention on Cyber Crime and its reflection in Judicial Decisions as well. Previously, the law solelyused to controlmechanism and administration searches of homes, containers and other corporal properties. In a world of corporealobstructions, activities that broke down those physical obstructions became the emphasis of judicial consideration. The world of digital search and seizure shows that this focus is conditional on the architecture of physical searches. As computer searches and seizures become more common in the future, one should see these basic set of laws that attains the basic objectives of adopting the changing aspects of searching physical property. Those physical laws will be coordinated by a frame of rules for digital searches and seizures that efforts to accomplish the similar purpose in a very diverse factual perspective.

The exposure-based method to digital searches:

It proposes a virtual version of the physical search approach: two shares a common definition of seizure, and both reject ex ante restrictions in war- rants.

The plain view doctrine:

At the same time, the shift to digital evidence should be accompanied by openness to rethinking other doctrines and addressing new questions, such as the proper scope of computer searches, the rules for

[70] Pt. 202 of *Supra* note 32.

searching copies, and the plain view doctrine, so as to update existing laws to reflect the environment of digital evidence.

The new world of computer search and seizure sheds new light and perhaps new scepticismon privacy-based focus.

The idea of privacy suggests that; privacy should be best seen as a vital byproduct of Information Technology Laws, not its aim. The viewpoint of computer search and seizure proposes that the in depth role of I doctrine is regulating the information flow between individuals and the state. In a sense, the digital world of computer data is a mainly pure policy for the Information Technology Laws to operate: it offers an environment of pure data, and deliberates how the courts can limit and regulate law enforcement ac- cess to that data given the practical dynamics of how the data can be retrieved. Privacy can be intruded when the lawlimitadmittance or usage of that information, but the wider question is how to control government access to information. The dynamics of criminal investigations in physical space support one set of answers to this question. The dynamics of investigations involving digital evidence may support another.

Acceptance procedures that are connected to the search and seizure of computer data put in storage in the similarway is required as with old-stylecorporal property. The requirements and the extent ofconfidencenecessary for the lawfulapproval are alike, nonetheless the situation is diverse. System storage dataor information storage channels may only be searched with the help ofsystem tools or through ICT systems. If the data required is put in another storage system, the search shall be long-drawn-out to the other system.

Methods should be accepted to seize or likewiseto safeguard the system info which has been investigated or accessed; this comprises seizing or in the same waysafeguarding the system or a portion of it, or the system info put in a storage channels itself. Law implementation shall be able to do and maintain a duplicate of the system info, and preserve the reliability of the data put in a storage. Besides at the similar time render inaccessible or eliminate the system data through the access gained to computer system.

Provisions should also permit the authorities to direct any individual who has informationregarding the working of the system or procedures made applicable to safeguard the system info therein to deliver, as is practical, the essentialmaterial to permit the responsibility of the search and seizures. But it should be assumed as restricted to give in to the material.

Some Common Investigation Mistakes which can occur during the process of investigation while collecting digital evidence are as follows:

1. Failure to collect and preserve the electronic evidence
    - The electronic files which are part of ‘captured’ computer, devices or media are isolated in a sanitized environment.
    - The replica/mirror image of the hard disks of computers, which have been seized by the investigating authorities to be deposited with the court.
    - The Hon’ble Court may take an appropriate decision with regard to such replica/mirror image would also be supplied to the accused under s.207 of Cr.P.C.,
2. Failure to label the electronic devices/media etc.

3. Failure to calculate the hash function*[or value?]* of the collected electronic data.

4. Failure to record details of computer forensic examination(s) in the charge sheet may lead to discharge or even acquittal of the accused.

From the above study following general recommendations are also drawn:

a. Search Seizureand Investigation Law should have a provision that requires those executing theauthority to search system tospecify in a search warrant that "we want anexactkind of data from the specific system.
b. The varied range of Administrative agencies should not be allowed to enter into private places even with a warrant. Yet again, it isessential for every agency to execute thisauthority should be according to the fair procedure established by law through a specific legislation.
c. Search Seizure and InvestigationLaw should specify thatmerely those persons doubted of being straightaway engaged inillegalactions should be exposed to investigation orders.

d. Search Seizure and InvestigationLawshould specify thatmerely those individualswho are straight away engaged in criminal actions should be mandatorilygive accessto the stored data in computer systems.
e. Agencies accountable for executing strip searches should be held liable for notabiding with theguiding principle. Failure of the person executing the search to follow with guidelines should render the search unlawful and any proofacquiredinacceptable.
f. Search Seizure and InvestigationLaw should permit privilege holders to protectrightsof the freedom before a Judge. A Court should decide,if thedata has been ready, collected or arranged for a deceitfulobjective.

Summary:

Information Technology Law coupled with the physical laws governing the issue of Search, Seizure and Investigation is developing as the judgesareadopting different approaches in deciding the cases to match up with thenovelrealisticcircumstances which are rising in a time of increasing computer usage. The courts are dealing with the issue on how the establishedprinciples in law relating to search and seizure law should be made applicable in the perspective of computer searches. This module studiesthe application of developing law relating to the Search, Seizure and Investigation in Cyber Space at national, regional and international law to the court determinations on questionsinterconnected to the inclusions and exclusions to the warrant requirements; when computer system searches are problematic.