International Journal of Communication Networks and Information Security
2024, 16(S1)
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

Digital Evidence and it's Admissibility under the Indian Legal Regime

Richa Gupta[1,*], Prof. (Dr.) Puneet Bafna[2]
[1]Research Scholar, Amity Law school, Amity University Rajasthan
[2]Professor, Amity Law School, Amity University Rajasthan
* Corresponding author: Richa Gupta,Research Scholar, Amity Law school, Amity University Rajasthan

ARTICLE INFO
Received: 12 Aug 2024
Accepted: 19 Sep 2024

ABSTRACT

The advent of digital technology has revolutionized every aspect of modern-day society, including the judicial landscape. Often, technological advancements lead to an imbalance of power in favor of the party with the most access to technology and the most adept use of it in legal proceedings. This imbalance of power has a severe impact on the fairness of legal proceedings.

For instance, those who have access to the most up-to-date technology are in an advantageous position to collect, analyze, and present evidence more effectively and efficiently than those who do not, giving an unfair advantage in the courtroom.

Electronic records/ digital evidence is increasingly presented and accepted in courts without scientific validation of the digital forensic methodology or tools. While classical investigative measures are subject to strict limits and fair trial guarantees, digital investigations still lack quality assurance and accountability. There are no minimum standards for digital evidence to establish and enforce scientific validation in digital forensics.

In addition, digital advancements like Chat GPT have allowed for the introduction of automated systems that can analyze and interpret legal documents. These automated systems are often able to make decisions and render judgments more quickly than human lawyers, and they can often do so with less bias. This has led to an increase in the number of cases being decided by automated systems, which can lead to more unfair outcomes.

Contemporary criminal investigation assisted by computing technology imposes challenges to the right to a fair trial and the scientific validity of digital evidence. Admissibility of an evidence is a very crucial stage in any civil/criminal trial and substantially effects its outcome. Technological advancements keep on presenting new and unique challenges before the courts and judiciary by offering the various new forms of electronic evidences.Another challenge that is faced in regards to electronic evidence is the ease with which it can be forged, fabricated, and manipulated and makes it all the more difficult to decide about the admissibility and veracity.

The varied type of electronic evidence such as email, instant chat messages, SMS/MMS,
communication made on social networking platforms; data stored on hard disk/ memory card
CD, DVD, browsing history on search engines, etc. poses unique problem and challenges for proper authentication and subject to a different set of views.

This paper seeks to trace the changing legal regime regarding admissibility of digital/e-evidence with special reference to Search and seizure of digital evidence and its interaction with right to privacy as recognised under Indian constitution.
Keywords: Digital Evidence, Admissibility, Search and Seizure, Right to Privacy

India was home to 467.0 million social media users in January 2023, equating to 32.8 percent of the total population. A total of 1.10 billion cellular mobile connections were active in India in early 2023, with this figure equivalent to 77.0 percent of the total population[1]. This outlines the enormous growth in e-governance throughout the public and private sectors. The Government anciencies are also opening up to introduce various governance policies electronically leading to the evolution of electronic records and evidencesas a fundamental pillar of communication, processing and documentation.

The relevant legal provisions dealing with the admissibility are broadly contained in Indian Evidence Act, 1872 and Information Technology Act, 2000 (hereinafter referred to as IT Act)

It is not that before the IT Act electronic records/ Digital evidences were not admissible. The kind of technology and evidence used today were far from anticipation when the Evidence act was enacted but with few amendments it still holds good and after the enactment of Indian Technology Act, 2000 the Evidence Act was correspondingly amended by virtue of Sec 92 of IT Act.

Position before Information Technology Act 2000

Before the enactment of Information Technology Act, 2000 any kind of "electronic records/ Digital evidence collected through all means including through cyber forensics was considered as a document and secondary evidence of these electronic "documents" was adduced through printed reproductions or transcripts, the authenticity of which was certified by a competent signatory. The signatory would identify his signature in court and be open to cross examination"[2]. All these was done in accordance with the conditions mentioned under sections 63(2) read with Sec 65(d) of the Evidence Act, 1872.

> "63. Secondary evidence. –– Secondary evidence means and includes ––
> (1) xxxxx
> (2) copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies;
> 65. Cases in which secondary evidence relating to documents may be given.––Secondary evidence may be given of the existence, condition, or contents of a document in the following cases: ––
> (a) xxxxxxxx
> (b) xxxxxxxx
> (c) xxxxxxxx
> (d) when the original is of such a nature as not to be easily movable;"

Position after Information Technology Act 2000

The Information Technology Act, 2000 was enacted by the Indian Parliament in 2000. It is the primary law in India for matters related to cybercrime and e-commerce. The act was enacted to give legal sanction to electronic commerce and electronic transactions, to enable e-governance, and also to prevent cybercrime. Accordingly Indian Evidence Act, 1872 was amended by virtue of Sec 92 of IT Act, 2000 (Before Amendment). The relevantprovisions for this paper are discussed hereinafter.

Section 3 of the Evidence Act was amended and Phrase "All documents produced for the inspection of the court" were substituted by "All documents including electronic records produced for the inspection of the court". Regarding the documentary evidence, in Sec 59, for the words "contents of documents" the words "Contents of documents or electronic records" have been substituted and Sec 65A and 65B were inserted to incorporate the admissibility of electronic evidence/ records.

The Information Technology Act defines the words' Electronic Record' under section 2(1) (t) as

> "–electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche;"

[1]://datareportal.com/reports/digital-2023-india#:~:text=The%20state%20of%20digital%20in%20India%20in%202023&text=India%20was%20home%20to%20467.0,percent%20of%20the%20total%20population.

[2]Dubey V. Admissibility of electronic evidence: an Indian perspective. Forensic Res Criminal Int J. 2017;4(2):58-63.

According to Cyber Centre[3], "digital evidence means any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device". Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence. Digital evidence is defined as: "any information processed by electronic medium which supports or refutes a hypothesis about the state of digital artefacts or digital events, of potential relevance and probative value for a criminal investigation"[4]. Digital evidence is the result of scientific methodologies and tools which ensures that "*its authenticity and integrity can be validated"*[5].

Given our contemporary lifestyle electronic records/digital evidences have acquired an omnipresent character. It can be found on our smart phones and computers, tablets, routers, hard-drive/flash-drive, cameras, Internet-enabled home appliances (e.g.,smart televisions, washing machines and refrigerators), and gaming consoles (to name a few), cloud storage of devices used by the user, history of user activities and other private resources. Electronic evidences/ digital records are also available on public platforms (e.g., social media platforms, websites, and discussion forums). The records and data of single user can thus be traced and stored wholly or in fragments by many different providers in servers in multiple locations[6].

According to Sec 2 of the Evidence Act, the word 'Evidence' means

> **"Evidence."**-- "Evidence" means and includes--
> (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry;
> such statements are called oral evidence;
> (2)[all documents including electronic records produced for the inspection of the Court;]
> such documents are called documentary evidence.
> The word 'Document' means
> **"Document."**-- "Document" [4]means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter".
> Thus, the word document means anything used for the purpose of recording a fact and correspondingly now includes CDs, Hard drives, Memory Cards, pen Drives etc.

The rules and procedure regarding the admissibility of electronic records are contained in newly inserted provisions of Sec 65A and 65B of the Evidence Act. These two provisions form a complete code for determining the conditions for admissibility of electronic/digital records and has been a source of lot of jurisprudence.

"Section 65A. Special provisions as to evidence relating to electronic record-The contents of electronic records may be proved in accordance with the provisions of section 65B[7].

Section 65B Admissibility of electronic records

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:--

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation

[3]Cyber Centre is a collaborative project of the International Association of Chiefs of Police (IACP), the National White Collar Crime Centre (NW3C) of United States, and the Police Executive Research Forum (PERF). Website: www.iacpcybercenter.org

[4] https://doi.org/10.1016/j.clsr.2021.105575

[5]https://www.sciencedirect.com/science/article/pii/S0267364921000480

[6] https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

[7]Ins. by Act 21 of 2000, s. 92 and the Second Schedule (w.e.f. 17-10-2000).

during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.
(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether--
(a) by a combination of computers operating over that period; or
(b) by different computers operating in succession over that period; or
(c) by different combinations of computers operating in succession over that period; or
(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,
all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, -
(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate,
and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
(5) For the purposes of this section,
(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment; --
(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.
Explanation. -- For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process."
A careful reading of Section 65B outlines the both technical and non-technical conditions for admissibility of a secondary evidence (duplicate copy including a print-out) produced from an original electronic record.
While Subsection (2) lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be submitted before the court; sub-section (4) provides for the non-technical condition i.e. mandatory requirement of a certificate of authenticity, signed by a person occupying a responsible official position ensuring the compliance of conditions stated under sub-section (2).

"a) The computerthat is used to produce or create electronic record must be in regular use;
b) The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer;
c) The computer was operating properly; and,
d) The duplicate copy must be a reproduction of the original electronic record"[8].

"The certificate must identify the electronic record containing the statement, describe the procedure by which it was produced, and also specifies such particulars of any device involved in the production of the electronic record as may be appropriate for the purpose of showing that the electronic record

[8]https://www.mondaq.com/india/trials-amp-appeals-amp-compensation/944810/use-of-electronic-evidence-in-judicial-proceedings

was produced by a computer. The certificate must also deal with any of the matters to which the conditions for admissibility relate"[9].Thus, any electronic record/ digital evidence printed on a paper, or recorded, copied or stored in optical or magnetic media produced by a computer, if duly proved in the manner provided in sec 65-B, can be regarded as credible evidencein any civil or criminal trial. However, it is important to bear that a certificate under section 65B makes the electronic record/digital evidence only admissible, it does not prove that its contents are true.

The journey of existing legal regime can be traced through various precedents spread over a period of around two decades wherein the Judiciary have also demonstrated perceptiveness towards the intrinsic 'electronic' nature of evidence, which includes insight regarding the admissibility of such evidence, and the interpretation of the law in relation to the manner in which electronic evidence can be brought and filed before the court.Most of the cases have been revolving around the questions whether Certificate of Sec 65B is mandatory for admissibility of any digital/ electronic record; who can give such certificate etc.

In *State (NCT of Delhi)* v. *Navjot Sandhu alias Afsan* Guru[10](famously known as Parliament attack case)the Supreme court held that Section 65A uses the word "may" and therefore prescribes one of the ways that may be used to prove an electronic evidence/record. The provision does not use the word "shall" and makes it mandatory. The court further held that according to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies". "Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the Court. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge. Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 & 65.It may be that the certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65"[11].

This view of the Hon'ble Supreme Court held the field for eleven years till it was overruled in the case of *P.V. Anwar* V *P.K. Basheer & Others*[12], wherein the Supreme court observed that don't read the word 'may' in sec 65A rather read the word 'notwithstanding' in the beginning of Sec65B which gives an over-riding effect to the Sec 65A and 65B and therefore electronic evidence cannot be proved unless the procedure of sec 65B is complied with. The Hon'ble Supreme court observed that Sec 65A is only an introductory provision to Sec 65B and does not control it. "The certificate required under Section 65B (4) is a condition precedent to the admissibility of evidence by way of electronic record and any secondary evidence of electronic records is inadmissible unless requirements of Section 65B are satisfied:"Proof of electronic record is a special provision introduced under the EvidenceAct". The very caption of Section 65A of the Evidence Act, read with Sections 59 and 65B is sufficient to hold that the special provisions on evidence relating to electronic record shall be governed by the procedure prescribed under Section 65B of the Evidence Act. That is a complete Code in itself. Being a special law, the general law on secondary evidence under Section 63 and 65 must yield. An electronic record by way of secondary evidence therefore shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which the secondary evidence pertaining to that electronic record, is inadmissible"[13].

In *Shafie Mohamad* v *State of Himachal Pradesh*[14] the Supreme court agreed with the view taken in P V Anwar (Supra) but dwelled into a situation where electronic evidence is sought to be proved by a person who is not the in-charge of the device. For example, in a matrimonial dispute the husband

[9] Karia T. D., AkhilAnand and BahaarDhawan (2015), "The Supreme Court of India re-defines admissibility of electronic evidence in India", Digital Evidence and Electronic Signature Law Review, [Online: Web] URL: http:///www.journals.sas.ac.uk/deeslr/article/download/2215/2149

[10](2005) 11 SCC 600

[11] Ibid.

[12] (2014) 10 SCC 473

[13] Ibid.

[14](2018) 2 SCC 801.

wants to prove adultery against his wife and for this he seeks to produce the call records and messages from his wife's phone. In such a situation he cannot give a certificate under Section 65B because he is not the in-charge of his wife's phone.The division bench clarified that,"the requirements of the certificate under Section 65B (4) being procedural, can be relaxed by the court wherever the interest of justice so justifies, and one circumstance in which the interest of justice so justifies would be where the electronic device is produced by a party who is not in possession of such device, as a result of which such party would not be in a position to secure the requisite certificate"[15].

On account of the above-mentioned conflicting pronouncements the matter of *ArjunPunditrao Kholkar* v *Kailash Kushanrao*[16] was referred to the larger bench by the two-judge bench. Finally, a three- Judge bench of the Supreme court clarified the law regarding admissibility of electronic evidence and its observations can be summarised as follows:

The SC while upholding the PV Anwar (Supra) judgment and overruling the Shafie Mohammed's (Supra) Judgement made it clear that the certificate must be mandatorily provided as a condition under Sec65 B (4) for admissibility of electronic evidence. The major premise of Shafie Mohamad that such certificate can be dispensed with if the electronic record is sought to be presented by a person who are not in possession or in-charge of an electronic device, is wholly incorrect. All the efforts should be made to obtain the requisite certificate by the party u/s65B and if still the concerned authority refuses to provide such certificate or does not reply, then in such case the party can approach the court seeking production of such certificate from the concerned authority. Once such application is made to the court or when defective certificate is issued; the court will order/direct the concerned authority through summon to issue the requisite certificate. An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B (4) in cases in which such person refuses to give it. Recourse can be had to section 165 of the Indian Evidence Act, 1872 or Order XVI of the Civil Procedure Code, 1908 or section 91 of the Code of Criminal Procedure, 1973.

The court differentiated between 'original document' and 'content that may be treated as evidence of original document'. The original document is the original record contained in the computer in which original information has been stored whereas the latter refers to output of that very information that the computer gives.

The certificate as required under Sec 65 B is not necessary if the original document is produced as primary evidence. The owner of the respective electronic device be it PC, laptop, tablet etc. can provide it by stepping in the witness box and must prove that the device which he is producing contained the original information and that it has been operated by him. But where it is physically impossible to bring the device to be produced in the court the requisite condition of producing the document along with the certificate must be fulfilled.

The electronic evidence is required to be furnished before the trial is about to begin. If the accused desires to produce the certificate, then it shall depend on the facts and circumstances of the case as well as the discretionary power exercised by the court. As long as the hearing runs and the trial is not over yet then the court can direct, to produce the requisite certificate at any stage of the trial.

Search and Seizure of Digital Evidence

The provisions related to search and seizure are most important tools in the hands of the investigating agencies and confers very extensive powers on them. It is therefore but required that such powers should be exercised with due circumspection and discretion, and not to cause harassment of innocent persons. Presently the law relating to search and seizure is contained in Chapter VII of CrPC which lays the procedure along with the safeguards to be observed by investigating agencies. As the general rule, prior sanction of a court in the form of a warrant is required before a search. Section 93 allows a magistrate to issue a warrant for the search of any document or thingwhere he believes that there is a necessity of issuing a search warrant, otherwise the thing or document would not be produced and the production of same is required for the purpose of investigation. The particularity of the search warrant is not a requirement under Sec 93, and hence a warrant may authorise the general search of a place or it may specify a particular place or part thereof to which only the search shall extend[17]. Section 100 of CrPC,1973 provides for the search of a closed place along with the safeguards to be observed, such as requirement of a search warrant from the appropriate authorities, presence of witnesses, preparing a search-memo and giving a proper warning to the occupants before a police officer may be allowed ingress into the closed place.

However, there are exceptions to these general provisions and there are other provisions which give wide discretionary powers to both the magistrates regarding particularity of search warrant and to

[15] ibid

[16][2020] ibclaw.in 18 SC

[17] Section 93 CrPC, 1973

police for conducting search without warrant on the ground of necessity of preventing loss or fabrication of relevant evidence in a case[18].Although, an exception, a good number of recent cases indicate that this wide power is often used arbitrarily to circumvent due process of the law.

Again, the procedure of Search as prescribed in CrPC,1973 is premised on a single-step process: assuming that a warrant is issued or if the requirement is exempted, police can enter a place to be searched and retrieve property sought. However, the present legal regime fails to appreciate that search and seizure for electronic evidence/ digital record involves a dual process: at first the police conduct a physical search to seize digital hardware; and then the seized device is electronically search for the relevant data.

Any device seized contains tons of data ranging from What's app chat to one's private communication made with your doctor, lawyer or psychologist, college project and personal DVDs of wedding and birthday parties...The invisible characteristic of digital information, unlike any tangible object, results in law enforcement officers reviewing the personal and sensitive content on any digital media during the search and seizure process[19], inevitably resulting in violation of Right to Privacy which is now a Fundamental Right vide *Justice K S Puttaswamy (Retd.)* v *Union of India & others*[20] covered under Article 21 of the Constitution.

Another important aspect is that "under the Indian law, the admissibility of an evidence is independent to the legitimacy of procedure observed for procuring the evidence and falls on the extreme end of the spectrum as compared to most other countries. Indian courts have continued to hold that even if there was illegality involved in procuring the evidence, it was admissible and the legality of convictions based on illegal evidence remains unaffectedsubject to greater scrutiny by courts"[21].

Provisions under the Indian Legal Regime

There is a complete absence of procedure to beobserved while searching for digital evidence. What locations cannot be searched for the discovery of the device and what contents to be searched for? What electronic records can be searched and to what extent? What is the procedure for confiscation and seizure of an electronic record/ digital evidence and when such device should be returned. Unfortunately, there is no procedure or any guidelines in the Code of Criminal Procedure, 1973 and Information technology Act, 2000 except some piecemeal provisions.

Section 69 and 69B of the IT Act,2000 provides that any surveillance by interception, monitoring, and decryption of data can be done only for specific grounds like security of state, defence of India, relation with a foreign state etc., on an order of notified functionaries authorised by the central/state government. Further four set of rules were framed and incorporated under Sec 43A of the Information Technology Act, 2000 in 2011, containing several provisions related to the search and seizure of electronic record. For eg. Rule 3(9) of Intermediary Guidelines rules allows access to information from intermediaries on a written order by a legally competent authority for the purposes of facilitating any investigation, protection, cyber security or intelligence activity.

Rule 6 of the Security Practices Rules, 2011 authorises any government agency to obtain any personal data from an intermediate "body corporate" which stores such datafor the prevention, detection, investigation, prosecution, and punishment of offences.

By and large digital privacy under Indian law and policy has completely failed due to the surveillance of communications and governmental access to digital records of online communications (including emails, website logs, etc.) without judicial scrutiny and accountability[22].

In the case *Virendra Khanna* v *State of Karnataka and others*[23], the High court of Karnataka laid the detailed guidelines to be followed by investigating officers to be observed while conducting a search and/or for preservation of evidence gathered during an investigation that concerns digital evidences like smartphones, electronic equipment or email accounts. These guidelines may serve the purpose till the legislature lays the law in this regard.

"In the case of a personal computer or a laptop;

- When carrying out a search of the premises, as regards any electronic equipment, Smartphone, or an e-mail account, the search team is to be accompanied by a qualified Forensic Examiner.

[18] Sec 165 of CrPC, 1973

[19] https://www.sciencedirect.com/science/article/abs/pii/S1742287613000042

[20] AIR 2017 SC 4161

[21] R M Malkani V State of Maharashtra AIR 1973 SC 157

[22] S. 69 and 69B of the Information Technology (Amendment) Act, 2008.

[23] 2021 SCC OnLine Kar 5032

- At the time of the search, the place where the computer is stored or kept is to be photographed in such a manner that all the connections of wires including power, network, etc. are captured in such photographs.
- A diagram should be prepared to show the manner in which the computer and/or the laptop is connected.
- If the computer is powered on and the screen is blank, the mouse could be moved, and as and when the image appears on the screen, the photograph of the screen to be taken.
- The MAC address also to be identified and secured. In the unlikely event of the Forensic examiner not being available, then unplug the computer, pack the computer and the wires in separate faraday covers after labelling them.

Apart from the above steps regarding the seizure of the computer, laptop, etc., if the said equipment is connected to a network, the following was recommended:

- To ascertain as to whether the said equipment is connected to any remote storage devices or shared network drives, if so to seize the remote storage devices as also the shared network devices.
- To seize the wireless access points, routers, modems, and any equipment connected to such access points, routers, modems which may sometimes be hidden.
- To ascertain if any unsecured wireless network can be accessed from the location. If so, identify the same and secure the unsecured wireless devices since the accused might have used the unsecured wireless devices.
- To ascertain who is maintaining the network and to identify who is running the network – get all the details relating to the operations of the network and the role of the equipment to be seized from such network manager.

In case of mobile devices, the following was recommended:

- Mobile devices would mean and include smartphones, mobile phones, tablets GPS units, etc.
- Prevent the device from communicating to the network and/or receiving any wireless communication either through Wi-Fi or mobile data by packing the same in a faraday bag.
- Keep the device charged throughout, since if the battery drains out, the data available in the volatile memory could be lost.
- Look for slim-slots, remove the sim card so as to prevent any access to the mobile network, pack the sim card separately in a faraday bag.
- While conducting the search, if the investigating officer seized any electronic storage devices like CD, DVD, Blu-Ray, pen drive, external hard drive, USB thumb drives, solid-state drives, etc., located on the premises, label and pack them separately in a faraday bag.
- The computers, storage media, laptops, etc. to be kept away from magnets, radio transmitters, police radios, etc. since they could have an adverse impact on the data in the said devices.
- To carry out a search of the premises to obtain instructions manuals, documentation, etc., as also to ascertain if a password is written down somewhere since many a time person owning equipment would have written the password in a book, writing pad or the like at the said location.
- The entire process and procedure followed to be documented in writing from the time of the entry of the investigation/search team into the premises until they exit"[24].

Can a person be compelled to unlock his phone/laptop or disclose passwords

The Supreme Court in *State ofBombay v. Kathi Kalu Oghad*[25] held that the Right against self - incrimination under Article 20(3) of the Constitution extends exclusively to the knowledge personal to a person and does not extend to any mechanical process used to produce a document. The court clearly observed that no accused can be compelled to give evidence that may have the tendency to incriminate him. However, the court expressly excluded finger-prints and handwriting samples

[24] https://factly.in/important-court-judgments-about-guidelines-regarding-search-of-electronic-devices-independence-of-state-election-commissioner-etc/

[25] 1961 AIR 1808.

because of their integral character not capable of being changed. Also, such evidences can be used only for the purpose of corroboration. Balancing the rights of an accused vis-a vis need for effective investigation the Supreme court held that giving finger prints and handwriting samples falls beyond the scope of testimony and is not incriminatory in nature."The information only personal to the knowledge of the person is in the ambit of Article 20(3) and not any process of producing mechanical documents. No accused can be compelled to give any incriminating evidence against him but they excluded finger impressions and handwriting samples because of their inherent character that cannot be changed and that evidence can only be used for corroboration. A mere sample of handwriting or finger impressions is not incriminatory in nature. It was held that giving fingerprints and handwriting sample is beyond the limits of 'testimony' which includes oral and written shreds of evidence. The reason behind this was simply because it is necessary in some cases to take physical impressions of an accused of the purpose of fruitful investigation"[26].

Further, Supreme Court in *Selvi v. State of Karnataka*ha laid that "a zone of mental privacy is established by Article 20(3), which the State may not invade in order to obtain personal information concerning a crucial fact. Further, if statements may lead to incrimination by themselves or "furnish a link in the chain of evidence" the bar of Article 20(3) of the Constitution would apply"[27].Accordingly,Article 20(3) prohibitsonly 'testimonial compulsion' but the same can be surely used to corroborate or identify the evidences already known to the investigation authority.

The above judgments outline two important conditions viz.Firstly, as a rule an accused can be compelled to give only non-testimonial or physical evidence, and secondly such evidences are required only for corroboration or to establish a link in the chain of evidence. Here the question arises whether the accused can be compelled to unlock his/her phone from fingerprints to collect the other pieces of evidence which can be present in the phone.

The law is not settled on this point and has been a subject of divergent views by different High Courts. The Karnataka High court in Virendra Khanna (supra) has treated the fingerprints as non-testimonial evidence and hence an accused can be compelled under section 91 CrPC, 1973 to provide password in order to unlock his phone/laptop without violating the mandate of Article 20(3). However, a Special CBI court of Delhiin the case of *CBI* v *Mahesh Kumar Sharma*[28]has observed that a password is not a document under section 91 CrPC, 1973 rather it lies within the domain of personal knowledge of the accused, stored in his mental zone and therefore while compelling an accused to provide password to unlock his phone/laptop would be an invasion of his mental privacy as protected under Article 20(3) of the Constitution.

Conclusions and Suggestions

Science and law are two distinct professions that combine to ensure fairness and justice. The aboveanalysis clearly uncovers the how technological advancements have outpaced the justice delivery system in ways not much discussed. With the enactment of Information technology Act, 2000 and incorporation of suitable amendments in the Evidence act, 1872, the existing legal regime is tailored to accommodate the evolving scientific challenges. However, these are just the beginning steps and much needs to be done to accommodate any challenges that may arise in future. With the advent of artificial intelligence, it is now possible to manipulate the digital material at lightning speed forcing the law enforcement agencies and police to devote considerable time and resources to get acquainted with the ever-evolving technology and learn the mechanism to curb the same. We are in a compulsive state of shifting our investigation techniques from traditional to the latest modern technological methods to keep up with the changing times to make our justice delivery system really effective.

[26] ibid

[27] (2010) 7 SCC 263.

[28]2022 SCC OnLine Dis Crt (Del) 48.