INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | June 2023
ISSN: 2582-6433

DIGITAL FORENSICS IN INDIA: CHALLENGE OF PRIVACY IN HANDLING DIGITAL EVIDENCE

AUTHORED BY - BEVAN AVIL PINTO

Introduction

The word 'Forensic' is derived from Latin and refers to "of or before the forum." Forensic Science is mainly concerned with materials and indirectly through materials with men, places, and time[1]. In other words, the processing and identity of materials that establish the presence or absence of a link between the crime, criminal, the victim, the weapon of offense, the place, and the time of the occurrence can be referred to as Forensic Science[2]. However, despite the vast recent development in this field, Forensic Science has been used for decades, as can be referenced in History when medieval doctors would attempt to identify the cause of death. Nevertheless, in India, Forensic Science formally began with establishing the Central Fingerprint Bureau in Kolkata in 1897. Following this, the field of Forensic Science in India has been expanding with the development of Crime Laboratories, toxicology laboratories, chemical laboratories, etc. The importance of Forensic Science is seen in the modern day when direct evidence might not exist, but Forensic Evidence can prove the link between a crime and a criminal. In cases of homicide, suicide, or sexual assault, DNA profiling has been of immense help in identifying the perpetrators of a crime. The Significance of Forensic Science has also been established by the Supreme Court in ***Dharam Deo Yadav v. State Of Uttar Pradesh.***[3], wherein the court noted,

"In criminal cases, especially based on circumstantial evidence, forensic science plays a pivotal role, which may assist in establishing the element of a crime, identifying the suspect, ascertaining the guilt or innocence of the accused."

In the same case, the court also noted the types of crimes and their sophistication has been evolving, requiring stronger and more foolproof methods of Investigation and Forensic Science. This observation has been rightfully seen in the last two decades with the advent of the Internet and digitization. Everything, from documents to information, is going digital, increasing the range of crimes and their sophistication. Thus, in light of this, Cyber Forensics or Computer Forensics

[1] B. R. SHARMA, FORENSIC SCIENCE IN CRIMINAL INVESTIGATION & TRIALS (5th ed., Universal Law Publishing 2018).
[2] Dharam Deo Yadav v. State of UP, (2014) 5 SCC 509.
[3] Prachi Kathane, Anshu Singh, J.R. Gaur, & Kewal Krishan, *The Development, Status and Future of Forensics in India*, 2 FORENSIC SCI. INT'L (2020).

ISSN: 2582-6433

emerged in response to the increase in crimes committed by computer systems as a part of the crime. The term Digital Forensic can be defined as,

"The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."[4]

The amount of Digital Data available online is unimaginable to the World Economic Forum; by 2025, it is estimated that each day, nearly 463 exabytes of data will be created globally[5]. Sensitive data, such as passwords, financial information, and other personal details[6] are available online, and the loss of such data would drastically affect a consumer. Thus, Digital Forensic Teams need to be able to track down criminals online using computer systems to target citizens.

This paper shall first establish the various legislations and frameworks in India that deal with handling digital evidence and Digital Forensics at large. The paper then analyses the various challenges in handling Digital Evidence and Digital Forensics. Finally, the paper shall seek to establish the relationship between the Right to Privacy and Digital Forensics and how Digital Forensics can potentially violate the Right to Privacy of an Individual. The paper shall finally conclude on the importance of developing Digital Forensics and provide suggestions.

Digital Evidence in Indian Law

Forensic Science in India is not governed by a single law but is derived from a combination of laws. The three main legislations that govern the understanding of digital evidence and its relevancy and admissibility are from the Criminal Procedure Code, 1973[7] (CrPC), Indian Penal Code, 1860[8] (IPC) and Indian Evidence Act, 1872[9] (IEA). Notably, these laws are not exhaustive in the development of Evidence and Forensic Science. However, these laws are the most

[4] Rupali K.Kulkarni & Dr.A.D.Gawande, Digital Forensics, 5 INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN ENGINEERING RESEARCH 333 (2017).
[5] Jeff Desjardins, *How much data is generated each day?* WORLD ECONOMIC FORUM (Apr. 4, 2023, 4:34 PM), https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.
[6] The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 3, Gazette of India, pt. II sec. 3(i) (Apr. 11, 2011).
[7] Criminal Procedure Code, 1973, No. 2, Acts of Parliament, 1974 (India).
[8] The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
[9] Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India).

ISSN: 2582-6433

significant when dealing with forensic science. In the case of Digital Evidence, the Information Technology Act, 2000[10] (IT Act) becomes very relevant in dealing with the evolution of crimes to cyber crimes and is, thus, very relevant when dealing with digital evidence.

The IPC, IEA, and CrPC were drafted much before the issue of Digital Evidence came into existence; however, it was updated with several amendments and changes. However, it is vital to note that the IT Act's enactment gave rise to the understanding of Digital Forensics and Digital Evidence. The IT Act serves as the main focal point for understanding Digital Evidence.

The IT Act defines several words that are very important to understand for the collection of Digital Evidence. The Act defines "digital signature," "electronic record," "computer," "computer network," "computer system," "data," "information," and "intermediary" and establishes the legal recognition of electronic records and digital signatures. While it must be noted that the Indian Penal Code defines a Document as *"any matter expressed or described upon any substance employing letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter."*[11], however, the IT Act defines the term 'Electronic Record' as *"data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche."*[12]. Thus, there is a significant difference in the very definitions of the terms. In addition to this, the IT Act also provides for several crimes, such as unauthorized access to Computer Systems under section 43[13] and tampering with computer source documents under section 66[14] and also provides the government with the power over any information transmitted through a computer in the interest of the sovereignty, defense, security, or friendly relations with foreign states under Section 69[15].

Therefore, the IT Act provides a large framework for understanding the use of Digital Evidence. However, it must be noted that the IT act alone is insufficient and must be understood in light of the IEA. The very definition of evidence under the IEA provides "*all documents including electronic records produced for the inspection of the Court."*[16]. The Indian Evidence Act has been amended to provide for the relevancy and admissibility of Electronic Evidence before the Courts.

[10] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[11] The Indian Penal Code, 1860, §29, No. 45, Acts of Parliament, 1860 (India).
[12] The Information Technology Act, 2000, §2(t), No. 21, Acts of Parliament, 2000 (India).
[13] The Information Technology Act, 2000, §43, No. 21, Acts of Parliament, 2000 (India).
[14] The Information Technology Act, 2000, §66, No. 21, Acts of Parliament, 2000 (India).
[15] The Information Technology Act, 2000, §69, No. 21, Acts of Parliament, 2000 (India).
[16] Indian Evidence Act, 1872, §3, No. 1, Acts of Parliament, 1872 (India).

ISSN: 2582-6433

Under Section 45A[17] of the IEA, the opinion of the Examiner of Electronic Evidence is considered an expert opinion and is, thus, considered relevant facts under section 45 of the IEA. This read with CrPC section 293[18] regarding the reports of government experts showcases the importance given to the collection of Digital Evidence. Moreover, if the evidence in question is that of a Digital Signature, then the opinion of the Certifying Authority that issued the Signature would be relevant under Section 47A. However, it must be noted that in the case of **the State Of Himachal Pradesh v. Jai Lal**[19], the Supreme Court noted that the scientific opinion evidence becomes an important factor; however, the credibility of such a witness depends on the reasons for the conclusion drawn based on the data and materials furnished. Thus, it is important to note that although evidence may be in electronic form, the reasoning and conclusion of an Expert will determine the credibility of the expert and, in turn, the evidence.

In the case of **Mukesh v. State of N.C.T. of Delhi**[20], the CCTV footage of a nearby area was used to corroborate the story of the victim in a rape case. The Computer Cell Expert's Forensic Division Head of Department testified that there was no tampering with the CCTV footage. Thus, the court accepted the testimony of the expert in this regard.

Another important Section under the IEA is Section 65B[21] which largely discussed the admissibility of Electronic Records. This section provides that any information in an electronic record that is printed on paper, stored, recorded, or copied in optical or magnetic media shall be deemed a document and admissible as evidence in a court of law.

In regards to Section 65B of the IEA, the Supreme Court, in the case of ***Anvar P.V v. P.K. Basheer***[22], the court noted that primary sources of electronic records could be admissible without following Section 65B; however, Secondary Sources of Electronic Evidence are susceptible to being tampered with, and thus, the safeguards presented under Section 65B concerning the source and authenticity of electronic records are necessary in order to be used as evidence.

Similarly, in the case of **Vikram Singh v. State of Punjab**[23], the court opined that a tape-recorded

[17] Indian Evidence Act, 1872, §45A, No. 1, Acts of Parliament, 1872 (India).
[18] Criminal Procedure Code, 1973, §293, No. 2, Acts of Parliament, 1974 (India).
[19] State Of Himachal Pradesh v. Jai Lal, 1999 Supp(2) SCR 318.
[20] Mukesh v. State of N.C.T. of Delhi, AIR 2017 SC 2161.
[21] Indian Evidence Act, 1872, §65B, No. 1, Acts of Parliament, 1872 (India).
[22] Anvar P.V v. P.K. Basheer, AIR 2015 SC 180.
[23] Vikram Singh v. State of Punjab, AIR 2017 SC 3227.

ISSN: 2582-6433

version of which a ransom call was recorded would not come under secondary evidence and, thus, no certificate would be necessary under Section 65B.

Therefore, the IEA, IPC, CrpC, and IT Act of India form the main understanding of Digital Evidence in India and its reliability, relevance, and Admissibility. Thus, law enforcement agencies must understand the severity of Electronic Evidence as it is very susceptible to tampering, and careful measures are adopted in the collection of Digital Evidence.

Procedure for Collection of Digital Evidence

The procedure for collecting Digital Evidence is often similar to that of the Collection of Evidence from a Regular Crime scene. In Crime Scene Management, the dimensions of the crime scene and potential safety are first established. Following this, the Crime scene is then preserved, ensuring that it remains undisturbed until the Investigation Officer arrives. After the arrival of the Investigative Officer, the crime scene is recorded, sketched, and photographed. Post this, the search for evidence begins with the officers moving around the crime scene in a particular manner to find evidence for collection. Once the evidence is found, it is collected and preserved in a particular manner to ensure that the evidence cannot be destroyed or tampered with[24]. It must be noted that this method of Crime Scene Management is very similar to that of the Collection of Digital Evidence in Cyber Crimes.

In Digital Forensics, the first stage is the Assessment of the Crime Scene. In this stage, importance is given to obtaining the proper authorization to conduct a computer investigation. Assessment of the case, questioning the relevant parties, and logging results in order to identify the crime and evidence[25]. It is very important to assess the situation in a Cyber Crime as several types of cyber crimes can occur on a computer, such as logic bombing, identity theft, data manipulation, hacking, and so on. Thus, an investigation team needs to assess the cybercrime and the extent of the damage caused.

The second step is the Preservation Stage. Soon after the assessment of the digital crime that has taken place, the preservation stage begins. The Preservation of a digital crime scene essentially

[24] B. R. SHARMA, FORENSIC SCIENCE IN CRIMINAL INVESTIGATION & TRIALS (5th ed., Universal Law Publishing 2018).
[25] K.K. Sindhu & Dr. B.B. Meshram, *Digital Forensic Investigation Tools and Procedures*, 4 I.J. COMPUTER NETWORK & INFORMATION SECURITY 39 (2012).

ISSN: 2582-6433

refers to the freezing of the crime scene. Operations such as preventing the use of computer systems, stopping any ongoing process concerning the crime, such as removal of data, and deliberating on the most appropriate way to extract the data.[26]

Following the Preservation Stage is the Collection Stage. The first and foremost step is to identify the sources of data and thereafter collect the data from the sources. Commonly seen sources would include mobile phones, laptops, cameras, smartwatches, and so on. After the sources are then narrowed on, the collection of data is then planned based on the significance, volatility, and difficulty involved in the collection[27]. Evidence of a crime is most often seen in the storage devices in the source, such as a hard disk. After the evidence is then narrowed on, at the time of collection, possibilities of manipulation are eradicated, and a chain of custody is established. It is necessary that the authenticity and source of digital evidence is maintained as was laid down by the Supreme Court[28] and thus, it is possible that a chain of events in relation to the data can be acquired during the collection of data, and proper care and caution must be exercised at the time of collection of the Data.

The next stage is the Examination and Analysis Stage of the Digital Forensic Investigation. The examination refers to the proper and thorough examination of the evidence collected in relation to cybercrime. The outputs in an examination include metadata, log files, time stamps, and other relevant information useful for establishing the crime, suspect, and victim[29]. After this, the examined evidence is then traced, filtered and any hidden data is uncovered, after which a conclusion is drawn[30].

After the Examination and Analysis Stage, the final stage is the Reporting Stage. Under this stage, all evidence collected and analyzed is reported, and the data from the investigation is included within this report, along with records of time stamps and chain of custody. Thus, concluding the Digital Forensic Investigation of Cyber Crimes.

[26] Rupali K.Kulkarni & Dr.A.D.Gawande, Digital Forensics, 5 INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN ENGINEERING RESEARCH 333 (2017).
[27] *Id.*
[28] Anvar P.V v. P.K. Basheer, AIR 2015 SC 180.
[29] Rupali K.Kulkarni & Dr.A.D.Gawande, Digital Forensics, 5 INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN ENGINEERING RESEARCH 333 (2017).
[30] K.K. Sindhu & Dr. B.B. Meshram, *Digital Forensic Investigation Tools and Procedures*, 4 I.J. COMPUTER NETWORK & INFORMATION SECURITY 39 (2012).

ISSN: 2582-6433

The Right to Privacy in Digital Forensic Investigation

The Right to Privacy is considered one of the most important fundamental rights in Modern Day. Since the case of **Kharak Singh v. The State of UP**[31], the Right to Privacy was noted to be of immense importance even though it was not declared to be a Fundamental Right under Article 21. It was later in the case of **R. Rajagopal v. State of Tamil Nadu**[32] that the Right to Privacy was viewed to be a tort. The court also noted that the Right to Privacy was not absolute in this case, and there were exceptions to the same. Similarly, in the case of **People's Union for Civil Liberties v. Union of India**[33], the court noted that the right to make a call without any disturbance is considered under the right to privacy and cannot be taken away unless under the procedure established by law. However, it was only in **Justice K.S. Puttaswamy Vs. Union of India**[34], the Constitutional Bench comprising 9 Judges, declared the Right to Privacy to be an integral part of the Right to Life and Personal Liberty under Article 21 of the Indian Constitution.

The Right to Privacy is of growing concern in the Digital Age. This right has also led to the development of the Digital Personal Data Protection Bill, 2022[35]. This bill ensures that users have a right to control their data, and no one can utilize their data without the consent of the user. Furthermore, several rights have been provided to the owner of the data while also creating obligations on the processor of Data. The entrance of this bill and the whole Digital Forensic seems to be in question due to the importance of the Right to Privacy.

As established, Forensic Investigation results in Investigators collecting data from sources; however, if left unchecked, the data collected could potentially be irrelevant to a crime and could jeopardize the privacy of the owner of the data. While the aim of Data Privacy is to ensure the data of the owner does not fall into the hands of unauthorized people, Digital Forensics is concerned with finding all potential evidence pointing to a crime.

When Digital Forensic Investigators manually approach files and determine their relevance to the crime, there is a risk of privacy violations for the private files that are not considered to be evidence in a given case. However, at the same time, this step is increasingly necessary as until an

[31] Kharak Singh v. The State of UP, AIR 1963 SC 1295.
[32] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[33] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.
[34] K.S Putthaswamy v. Union of India, (2017) 10 SCC 1.
[35] The Digital Personal Data Protection Act, 2022 (India).

ISSN: 2582-6433

investigator determines and examines a file, the investigator will not be able to ascertain the relevancy of the data to a particular crime[36]. This results in a high risk to the privacy of individuals. Thus, there is an obvious risk to privacy and violation of Article 21 in the process of Digital Forensics. However, it must also be noted that the Right to Privacy is not absolute. Firstly, Article 21 in itself is not absolute and is limited by the procedure established by law[37]. However, it is to be noted that there exists no regulations or guidelines that are used for digital forensic investigations. However, in the Landmark Puttaswamy judgment, the Supreme Court noted that the Right to Privacy is not absolute. Any law or procedure taking away the Privacy of an Individual must follow a three-pronged test of Legality, Necessity and Proportionality.[38]

In terms of Legality, the CrPC provides for the procedure of investigating. In normal crime scenes, an investigation would include panchanamas and recording of the crime scene[39], however, in a Digital Crime Scene, this would be difficult to establish as Data is not tangible, and it would be practically impossible to use pathnames for the investigation.

In terms of Necessity, it is undoubtedly necessary for investigators to find and examine evidence to determine the crime and suspects. However, at the same time, it is impossible for investigators to determine the relevancy of data unless it is examined. Thus, the violation of privacy in most cases is necessary in order to determine the relevancy of the data collected.

Finally, in terms of proportionality, the Forensic Investigation would include collecting Data from the Crime scene and any other data that is needed outside the purview of the scene would and in possession of the owner would require a warrant of search from a magistrate[40].

However, despite the possibility of the three-pronged test being fulfilled, the Right to Privacy of individuals still remains to be in risk as it is possible that there could be potential misuse of power and investigation at the time of the investigation. However, there are no current regulations regarding the handling of Digital Evidence which creates a problem for the Right to Privacy of Individuals.

[36] Robin Verma, *Digital Forensics 2.0: an automated, efficient, and privacy-preserving digital forensic investigation framework*, INDRAPRASTHA INSTITUTE OF INFORMATION TECHNOLOGY DELHI (2018).
[37] INDIA CONST. art. 21.
[38] K.S Putthaswamy v. Union of India, (2017) 10 SCC 1.
[39] Criminal Procedure Code, 1973, §100, No. 2, Acts of Parliament, 1974 (India).
[40] Criminal Procedure Code, 1973, §93, No. 2, Acts of Parliament, 1974 (India).

ISSN: 2582-6433

Conclusion and Suggestions

Digital Forensics in India is becoming more and more important. Crimes are evolving, and the use of technology in crimes is inevitable. Every individual carries a mobile phone which can also contain important evidence; however, it is important for Forensic Teams to be able to safely extract the data from digital sources and handle the data properly. If the data is tampered with or destroyed, it could result in freeing a criminal into society. Hence, the importance of Digital Forensics is only increasing with the passing of each day. However, despite the importance of Digital Forensics, the risks of the violation of the Right to Privacy is imminent. While the Informational Technology Act of 2000 and the several amendments to the Indian Evidence Act, Criminal Procedure Code, and Indian Penal Code have allowed for the development of Digital Forensics in India, there exist no proper guidelines or regulations for Digital Forensic Investigators to collect data while ensuring the highest level of privacy to data subjects not a part of the investigation. While the Personal Data Protection Bill 2022 may help promote the value of privacy, its effects may not be seen in Digital Forensics. Hence, it is essential that a uniform guideline for the handling of Digital Evidence and Digital Forensic Investigation is drafted.

In light of the research presented above, it is vital that there is an urgent need to develop a uniform framework for Digital Forensic Investigation in India. Firstly, the framework needs to establish the proper stages and methods of collection of data from sources. In doing so, unnecessary and unconnected data can be separated from the data that is necessary for the investigation. This would ensure privacy for owners of unconnected data. Secondly, the collected data must only be read by authorized individuals, and no other person should be permitted access, thus reducing the risk of privacy. Finally, any data that is not necessary must be returned and/or destroyed so that such data cannot be leaked. In addition, it is also important to note that a chain of events must be kept so as to reduce any issues arising from the collection of Data. Moreover, Digital Forensics Teams can also incorporate the use of Artificial Intelligence and Machine Learning to segregate relevant evidence from irrelevant ones. This would enhance the privacy of users whose data has been collected. Thus, by incorporating these suggestions, Digital Forensics can continue to grow without the risk to the privacy of unconnected users.