The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

HASHED AND CHAINED, YET DOUBTED: RELIABILITY OF DIGITAL EVIDENCE IN THE ERA OF CYBERCRIMES

~ Rishav Das

ABSTRACT

Digital evidence has assumed the position of the backbone of the modern criminal justice system on account of the contemporary proliferation of cybercrime, yet several unaccounted factors pertaining to its alteration, duplication and even deletion has not been able to save it from being perpetually questioned on grounds of reliability. This paper examines the exact question by the synthesis of three recent scholarly studies, taking into consideration the narrative review of the legal and forensic dimensions of electronic evidence, the doctrinal study of the Indian criminal legal background, especially post-enactment of the Bharatiya Sakshya Adhiniyam (Hereinafter referred to as 'BSA') and the qualitative study of the legal standards and the practices of chain-of-custody across several jurisdictions. This paper attempts to make a distinguishing premise between 'admissibility', which serves as a threshold question and 'reliability', which serves as the weight deserved by an admission. It makes an analysis of the authentication, chain-of-custody, expert testimony, cognitive bias and cross-border collection and procedural fairness as the core factors for determining reliability. It also traces the evolution of Indian criminal justice's certification requirement ranging from section 65B of the Indian Evidence Act (herein after referred to as 'IEA'), 1872 to section 63 of the BSA, 2023. Another additional consideration discussed here is the re-moulding of forensic practice by Artificial Intelligence, Blockchain, Internet of Things and Deepfake Detection. The paper also advances an argument that reliability cannot only be secured by mere legal codification, rather ought to be matched by standardised forensic protocols, adequate laboratory capacity and judicial training. As a final declaration, this paper would also like to caution that some of the empirical data set and case-law related material upon which, due reliance has been placed, derive their source from secondary commentary and hence, should be read as being indicative.

Keywords: *Digital Evidence; cybercrime; reliability; admissibility; authentication; chain-of-custody; digital forensics; Bharatiya Sakshya Adhiniyam; blockchain; deepfakes.*

INTRODUCTION

The advent of digital technology has ushered in a huge transformation in the two main pillars of crime, that is, its commission and proof. Offences ranging from ransomware, financial fraud, identity theft and attacks on infrastructure, critical in nature are frequently carried out through networks that are interconnected, coupled with cloud services and mobile communications that, in all probability, leave behind innumerable electronic records, scattered across several national boundaries[1]. Such is the raging presence of technology that computer-drawn information along with those arising out of cell-phones, cloud services, social media platforms and surveillance systems now possess a routine usage in event recreation, perpetrator identification, intent establishment and for testing accounts of witnesses[2]. Specifically, viewing from the Indian kaleidoscope, cybercrime investigation turns decisively on a plethora of evidence such as WhatsApp Chat Exports, call-detail records and transcripts, UPI transaction logs, footage secured from CCTVs, cloud-stored documents and metadata.[3]

Just like the fact that the crown itself makes the King come closer to his death, the exact same qualities that characterize the useful nature of digital evidence, also constitute its fragile side. Electronic records are easily susceptible to modification, deletion, encryption and manipulation and hence, it becomes incumbent on the court to judge whether its authenticity and integrity is compromised[4]. With due consideration of the relevant facts, their arises a two-fold question before criminal courts across any jurisdiction in the field of evidence; first is that whether the evidence adduced by the parties can be considered at all, primarily revolving around the question of admissibility and the second is that whether the evidence hence admitted, is deserving of weight, which revolves around the question of reliability[5]. This paper bases its chief concern on the second question, although the two questions being intertwined, on account of the fact that the procedural gateways leading towards admissibility are itself designed meticulously enough to filter out unreliable material.

---

[1] Dipender Chhikara, *Cuber Crime and the Legal Challenges of Digital Evidence: Admissibility and Reliability,* 22 J. ASIA ENTREPRENEURSHIP & SUSTAINABILITY 123 (2026).
[2] *Id.*
[3] Sahil Sehrawat, *Digital Evidence and Cyber Crime Investigation in India: Issues of Admissibility, Authentication and Reliability,* 3 INTERNATIONAL JOURNAL FOR LEGAL REASEARCH AND ANALYSIS 1750, 1751 (2026).
[4] Chhikara, *supra* note 1, at 124.
[5] Sehrawat, *supra* note 3, at 1752.

It is pertinent to mention that despite the richness of the literature on this subject, it remains fragmented. An integrated perspective of legal analysis, forensic methodology and technological innovation is an absolute must for being able to comprehend the changes brought about in the existing evidentiary standards by technological change[6]. This paper caters to that exact need by drawing together three complementary studies including a review of the legal and forensic dimensions of newly ushered digital evidence[7], a doctrinal examination of the replacement of the IEA, 1872 by the BSA, 2023[8], followed by a qualitative study evidentiary reliability[9]. This paper is based on collection of primary data, but critically examines three papers against one another and attempts at fishing out those areas where the evidence falls short or becomes stronger and thereby establishes a coherent account of what makes evidence reliable and what undermines its worth.

CLEARING THE CONCEPTUAL FOUNDATIONS

Talking about the evolving nature of cybercrimes, it has assumed significant growth owing to the digitization of communication and public services and encompasses a plethora of acts including malware and ransomware attacks, online financial fraud, cyber espionage, identity theft and a variety of offences, the commission of which occurs through connected smart devices[10]. An abundance of electronic traces is hence generated from such acts which are capable of being deciphered only by forensic analysts. Moreover, the documentation of crimes which posses a span over a multi-jurisdictional base creates newly emerging technical complexities[11].

Arriving at the juncture of meaningful deconstruction of concepts, digital evidence may be understood as any data, information of record generated out of computer that holds the potential of being used for the provenance of facts in a legal setting[12]. Scholarship from India defines it in similar, if not the same, as data "stored, created or transmitted electronically" that holds the capability of supporting or challenging a fact in issue and that is extracted and preserved through a process involving science, combining computer science, cyber security and criminal

[6] Chhikara, *supra* note 1, at 124.
[7] *Id.* at 123.
[8] Sehrawat, *supra* note 3, at 1750
[9] Hafiz Omer Abdullah, *Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era,* 3 RESEARCH JOURNAL OF SOCIAL AFFAIRS 795 (2025).
[10] Chhikara, *supra* note 1, at 124.
[11] *Id.*
[12] *Id.*

investigation methodology[13]. Courts even require that authenticity, integrity and traceability be established before acceptance of evidence[14]. Digital evidence also marks its difference from physical evidence in the way its evidence can be tested. Digital artefacts are prone to alteration during acquisition or any other stage of transmission and receival, thereby mandating the integrity verification as an essentiality before judicial determination[15]. Quite contrary to a physical exhibit, a digital artefact may be altered with scanty visible traces which becomes the reason for the imperilment of admissibility even due to a microscopic record-keeping deficiency[16].

Digital evidence marks its origin from a diverse array of sources, including computers and laptops, smartphones, cloud services, surveillance systems and the most famous Internet of Things (herein after referred to as 'IoT'). It is pertinent to mention that each source raises its own independent and exclusive forensic consideration[17]. An IoT environment assumes particular challenges because of the fact that evidence may be located and spread across heterogenous devices or cloud environments[18]. A forensic investigation which is structured typically flows through identification, acquisition, preservation, examination, analysis, interpretation and presentation to the judicial authorities, and evidentiary integrity and compliance with legal requirements ought to be maintained at every phase[19].

DECIPHERING THE LEGAL FRAMEWORK GOVERNING ADMISSIBILITY AND REALIABILITY

It should be mentioned right at the outset, that digital evidence which is collected and used in accordance with the legal procedures possesses the same evidentiary value as evidence of traditional nature. The accepted principles mandate the evidence to be relevant, authentic and reliable and should be procured only through lawful means[20]. Owing to the fact that electronic data is so prone to being altered or reproduced, courts frequently look for scientifically vali forensic methods holding the capacity to verify the veracity of the evidence[21]. At the same time, it should be noted that the law is still in a nascent stage and still developing to strike a balance

[13] Sehrawat, *supra* note 3, at 1751.
[14] Chhikara, *supra* note 1, at 124.
[15] *Id.* at 128.
[16] Abdullah, *supra* note 9, at 795.
[17] Chhikara, *supra* note 1, at 124-125
[18] *Id.* at 124.
[19] *Id.* at 125.
[20] *Id.* at 126.
[21] *Id.*

between efficiency of investigations and the protection of individual rights in criminal proceedings[22]. The law of evidence also falls short in it consideration that its rules were designed, years before and that too, for physical material. The prevalent rules on relevance, authentication and exceptions concerning hearsay fail to accommodate the mutability of digital files and the nature of cloud-based storage. Resultantly, the courts have consistently been inclined towards the adoption of a divergent approach, producing inconsistent results even in cases constituting similar factual matrix.[23] Hence, scholars have frequently called for a more coherent framework that would, by its very nature, reduce such inconsistencies[24].

Talking about Authentication, it provides a confirmation that the electronic evidence is in its genuine form and has not been altered following its acquisition and its subsequent introduction as evidence. It involves a plethora of acts such as metadata validation, cryptographic hashing, forensic imaging, documenting the process of acquisition and validating the techniques of analysis used henceforth[25]. Considering the same subject from the Indian standpoint, its literature also stresses that sound methodology mandates the stringent requirement of original data to be preserved unaltered[26]. Nevertheless, authentication has assumed quite some demand in the contemporary times as the provenance of evidence increases in its complexity. Nowadays, courts are also increasingly confronted with so called “evidentiary materials” derived from leaked or hacked sources and hence, evaluating its lawfulness becomes a prerogative.[27]

Where specialised acquisition techniques or very complex analysis are involved, Expert Testimony and Scientific Reliability assume great importance, where, the reliability of such testimony is dependent on methodologies that have a sound scientific premise. The consequent evaluation of admissibility now depends heavily on an expert’s willingness and ability to be true to the judicial process and demonstrate methodological transparency and his or her act of abiding by the accepted forensic practices[28]. It must be appreciated that this scrutiny that the courts apply as a standard, resonates with that established in Daubert v. Merrell Dow Pharmaceuticals, Inc[29], where authentication, error rates and methodological transparency have

[22] *Id.*
[23] Abdullah, *supra* note 9, at 796.
[24] *Id.* at 797.
[25] Chhikara, *supra* note 1, at 126
[26] Sehrawat, *supra* note 3, at 1759.
[27] Chhikara, *supra* note 1, at 126
[28] *Id.* at 127.
[29] *Daubert v. Merrell Dow Pharmaceuticals, Inc*, 509 U.S. 579 (1993).

become core factors of concern.[30] The same expectation can be viewed in government proposals securing accountability at every phase of digital evidence processing and evaluation[31]. Yet, placing heavy reliance on experts also comes with its own set of risks as it can obviously lead to biasness and variations in interpretations and also underscores the requirement of a continuing dialogue amongst lawyers and IT specialists so that the courts can assess the probative worth of electronic materials[32].

On account of the transnational nature of cybercrime, national laws on digital evidence ought to evolve in the same pace as technology. Divergent data protection laws, privacy laws and criminal procedures often tend to complicate the picture, for which, comparative studies nowadays focus on the harmonisation aspect through international cooperation. Contemporary developments such as the European Union's electronic evidence framework, have reduced to some extent, the uncertainty involved procurement of such evidence, yet majority of the difficulties remain[33]. On this account, it is pertinent to mention that reliability is not bounded to being a technical notion, but also a normative one grounded in a consensus of legal principles[34].

THE SHIFT IN THE INDIAN FRAMEWORK

The Indian position on electronic evidence was dominated for two decades by Section 65B of the Indian Evidence Act, 1872, owing its insertion to the Information Technology Act, 2000[35]. This provision mandated the requirement of a certificate of identification for the electronic record, with a detailed description of the manner of its production and a further detail of the device used and also made it incumbent on the person possessing the device or having a relation with it, to sign such a certificate. In this regard, it can be said that two Important Supreme Court decisions influenced its operation. In Anwar P. V. v. P. K. Basheer[36], the court held that an electronic record can be proved only abiding by Section 65B and that the certificate under sub-section 4 was a "mandatory pre-condition" for secondary electronic evidence to hold the status of being admissible[37]. Secondly, in Arjun Panditrao Khotkar v. Kailash Kishanlal Gorantyal[38],

[30] Abdullah, *supra* note 9, at 796.
[31] Chhikara, *supra* note 1, at 127.
[32] Abdullah, *supra* note 9, at 797-798, 802.
[33] Chhikara, *supra* note 1, at 127-128.
[34] Abdullah, *supra* note 9, at 798.
[35] Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872, § 65B (India) (repealed); Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); *see* Sehrawat, *supra* note 3, at 1757
[36] Anwar P. V. v. P. K. Basheer AIR 2015 SC 180.
[37] Sehrawat, *supra* note 3, at 1753-1754.
[38] Arjun Panditrao Khotkar v. Kailash Kishanlal Gorantyal AIR 2020 SC 4908.

it was held by the Supreme Court that the relaxation of rule of mandatory certification, as was mentioned in Shafhi Mohammad v. State of Himachal Pradesh[39], was incorrect and thereby restored the mandatory character of certification even upon production of the original device[40].

The Bharatiya Sakshya Adhimiyam, 2023 came into force on 1 July, 2023 whereby it replaced the IEA, 1872. Section 61 of the BSA provides that an electronic record shall not be denied admissibility on account of it being 'electronic'. Section 62 stipulates that its contents are to be proved in accordance with Section 63, which followingly sets out the certification requirements and mechanics[41]. In the view of the practitioner commentary, as reported in the study conducted in India, a certificate has been described as a standardised Schedule in two parts – Part A, which deserves completion from the person in charge of the device and Part B, which deserves completion from a technical expert, who is compelled to disclose the hash-value and a corresponding report, frequently called as the 'hash-report'[42].

CHAIN OF CUSTODY AND FORENSIC INTEGRITY

A seamless chain of custody is an absolute essential to both the integrity and credibility of digital evidence. Each and every step of collecting, storing, examining, transferring and presentation of the evidence ought to be documented in order to adduce as a proof of a material free from contamination[43]. Popular literature describes such a chain as a meticulous, unbroken record of every person who has handled an item, having a typical involvement of secure evidence-locker storage and a complete handling log pending transmission to a forensic laboratory or empanelled expert[44]. The importance of standardised retention and documentation practices assume particular importance owing to the increasing dependence of communication on metadata and electronic records[45]. Even in case where the data is technically admissible, the failure in the act of establishing a verifiable chain often leads to the only conclusion of suppression of evidence[46].

Technology offers some amount of assistance as well. Blockchain based chain-of-custody systems can help in the creation of verifiable history, that is independent of the vendor and can

[39] Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801.
[40] Sehrawat, *supra* note 3, at 1754.
[41] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023, §§ 61–63 (India); *see* Sehrawat, *supra* note 3, at 1754.
[42] *Id*. at 1754, 1758.
[43] Chhikara, *supra* note 1, at 126.
[44] Sehrawat, *supra* note 3, at 1759.
[45] Chhikara, *supra* note 1, at 126.
[46] Abdullah, *supra* note 9, at 797.

also aid in making tampering harder, thereby improving the procedure of transparency[47]. Though cross-jurisdictional studies record similar proposals, it notes unresolved concerns about costs, scalability and the courts' willingness to appreciate and in turn, accept technologically complex solutions. The only conclusion that could be arrives at was that it is only through the combined effect of technological efficiency and procedural transparency that success can be achieved in this field[48].

SYSTEMIC CHALLENGES FACED BY REALIBILITY

First of all, talking about human factors and cognitive bias, despite technical methods receiving one of the utmost importance, human judgment remains essential to the interpretation and reporting of evidence. Certain aspects such as cognitive bias, contextual information, confirmation bias and the existence of preconceived notions might cast a heavy influence on the investigators and this becomes even more obvious when dubious artefacts or a considerable volume of disparate data is examined by the analysts. However, it is only through standardised analytical procedures, independent verification and decision-making which is structured, that can cause a reduction in the magnitude of such subjective influence. Moreover, unequal access to resources and institutional expertise may also indirectly affect the collection of digital evidence and its subsequent interpretation[49].

Secondly, open-source intelligence coupled with online repositories and various cloud-based platforms have proved their value in cybercrime investigations, yet these being taken from publicly available spaces, undermines their worth on account of the probability of being manipulated or impersonated. Systematic integrity verification procedures and special mitigation strategies that are standardised are therefore, the need of the hour. Coupled with that, 'expert interpretation' has grown to be increasingly important where the technical authenticity of online evidence in under dubious consideration[50].

Thirdly, talking about the gaps in the institutional capacity, it needs to mentioned right at the outset that the Indian Study documents a two-tier laboratory structure consisting of the Government Forensic Science Laboratories and the Central forensic Science Laboratories. Numbering at approximately twenty-seven state and seven central laboratories, they enjoy the greatest credibility, but are nerfed by the typical turnaround times of forty-five to one hundred

[47] Chhikara, *supra* note 1, at 128.
[48] Abdullah, *supra* note 9, at 797.
[49] Chhikara, *supra* note 1, at 128.
[50] *Id.* at 128-129.

eighty days, owing to immense backlogs. Quite to the contrary, Private Laboratories, working under the Ministry of Electronics and Information Technology offer comparatively faster turnarounds between a staggering five to thirty days. Their admissibility credibility, though not equivalent to the former, still remain comfortably high[51]. The predicament of the victim follows here as well as they cannot approach the Forensic Science Laboratories in the absence of a registered FIR (First Information Report) and a subsequent request from the Investigating Officer (IO), which acts a further bottleneck[52]. Naturally, these constraints associate themselves with very poor outcomes. India's cybercrime conviction rate is even below eighteen percent and such a statistic is attributable directly to the lack of prosecutable evidence and extremely poor digital chain-of-custody practice, which never achieves satisfaction[53].

Fourthly, introducing the concept of cross-border collection, investigators might often find themselves under the obligation to extract evidence whose locations are found to be in other jurisdictions. As has been noted earlier in the paper as well that the differing standards of procedural rules, evidence-gathering and mutual legal assistance arrangements acts as a major hindrance to cooperation, thereby calling for harmonised procedures that do not compromise on preserving legal safeguards[54]. From the Indian perspective, it would be essential to mention that compliance requirements imposed by foreign-headquartered platforms have caused a significant delay in information exchange. Further, from the international relations perspective, India's non-membership of the Council of Europe's Budapest Convention on Cybercrime, further acts as a hurdle to the speed of cross-border cooperation and the reliability it poses[55].

Fifthly, ushering the concepts privacy, due process and procedural fairness, advanced visualisation, digital reconstruction and automated analysis generate pertinent legal as well as ethical question concerning the same topics. Excessive reliance on such reconstructions with non-disclosure of the underlying limitations, unduly influences the court's decision-making. It henceforth, becomes incumbent on the courts itself to assess the reliability and evidentiary value of such technologically enhanced material before jumping into the question of admissibility[56]. Courts have contemporarily employed a sensitive approach to 'surveillance

[51] Sehrawat, *supra* note 3, at 1756, 1760.
[52] *Id.* at 1760.
[53] *Id.* at 1761.
[54] Chhikara, *supra* note 1, at 129-130.
[55] Sehrawat, *supra* note 3, at 1761.
[56] Chhikara, *supra* note 1, at 130.

evidence'. Courts have acknowledged that reliability is not only bounded to being a matter of technical protection against error, but also of the inherent fundamental rights and due process[57].

EMERGING TEHNOLOGIES DECIDING THE FUTURE OF REALIABILITY

It is true that the advent of Artificial Intelligence (AI) and Machine learning (ML) has made the landscape of forensic investigation more traversable. It has not only made investigation faster, but also more efficient by introducing a reduction in the quantifiable extent of files requiring manual processing and identification of artefacts that may sabotage the human eye and prioritize them for analysis. These tools assume greater relevance in the fields of cybercrime involving complex data sources and attack techniques and they also render their assistance in international investigations through image analysis, recognition of objects and finding of correlation among evidence[58]. Yet, the only legal difficulty that arises even in the sector of Intellectual Property Rights is 'algorithmic transparency'. Simply put forward, a tool unable to self-explain its output, has very scanty chances of being reconciled with the absolute demand for methodological transparency. Therefore, the review identifies only those forensic algorithms that are explainable, as a research priority[59].

Secondly, comes the topic of Blockchain and the Internet of Things (IoT). Blockchain holds the capacity to document step-wise advancements of the lifecycle of the evidence, quite transparently, since records are immutable and time-stamped, thereby causing a reduction in the overall possibility of tampering. If we go down the lane of history, earlier block-chain based forensic models demonstrated a secure management of evidence, realised through verification which was decentralised by nature and later on, such approach was extended to IoT environments and also to multimedia evidence[60]. Various IoT devices such as wearables, smart homes, connected vehicles, etc, generate evidence that is of invaluable nature, but the collection procedure can be easily complicated by heterogeneous architectures and limited storage. At the current grounding, selective acquisition and data-reduction techniques are needed, which would help in the preservation of relevant information without any compromise in its reliability and preservation frameworks, combining blockchain, distributed storage and smart contracts showcase promise for securing IoT generated evidence[61].

---

[57] Abdullah, *supra* note 9, at 802.
[58] Chhikara, *supra* note 1, at 130.
[59] *Id.* at 131-132.
[60] *Id.* at 131.
[61] *Id.*

Thirdly, Deepfake and Synthetic Evidence technology poses itself among one of the greatest threats to the concept of reliability of evidence in the contemporary world. An automated risk, that the investigators and the courts would fall into the trap of being deceived, is generated merely because of the capacity to produce artificial images, audio and video, that act as a simulation of a real person or persons, with uncanny realism. Though media forensics has sharply responded back with automated detection of inconsistencies in visual, metadata and acoustic properties, it is suggestive that a combination of both human and machine-based detection strategies would be beneficial than either standing alone[62]. After studying Indian evidentiary jurisprudence, a more fundamental gap could be located, that neither Section 65B jurisprudence of the erstwhile Indian Evidence Act (IEA), 1872, nor Section 63 framework of the current Bharatiya Sakshya Adhiniyam (BSA), 2023 has addressed or made any consideration pertaining to the authentication of AI-generated or synthetically-doped material. This becomes prima facie more evident considering that the hash value only sends a confirmation of the unchanged nature of a file following the time period of its acquisition, but remains oblivious and silent on the issue of the authenticity of the material or the content.

RECOMMENDATIONS

Arriving at a rendezvous ground, the various studies converge on a set of reforms to ensure that digital and forensic evidence remains reliable and usable across various jurisdictions. The reforms focus on a potential standardization of forensic procedures through chain-of-custody procedures that are uniform in all respects[63]; clarification of legal standards with respect to qualifications of experts, the distinguishing factors between directory and mandatory rules and authentication of synthetically generated content[64]; expansion of institutional capacity by the resultant upgradation of state labs;[65] enhancement of training and collaboration so that judges, advocates and the police can work in tandem in the evaluation process of the evidence[66] and last, but not he least, fostering a sense of international coordination through harmonization of cross-border standards[67].

[62] Chhikara, *supra* note 1, at 132.
[63] Abdullah, *supra* note 9, at 803; Sehrawat, *supra* note 3, at 1765.
[64] Sehrawat, *supra* note 3, at 1764-1765.
[65] *Id*. at 1765.
[66] Sehrawat, *supra* note 3, at 1765; Abdullah, *supra* note 9, at 803.
[67] Chhikara, *supra* note 1, at 132; Abdullah, *supra* note 9, at 803.

CONCLUSION

Digital Evidence has now become an indispensable part of the broader picture of investigation and prosecution of cybercrimes, but what many people fail to understand is that its worth and value, both depends upon the amount of confidence it can inspire upon the courts, when placed before it. Specifically speaking, the three studies examined in this paper render the core information that reliability is not a single-factor determination, rather it is built over a combined premise of legal norms, scientific methods and institutional capacity. Genuineness, integrity and strong chain-of-custody protocols remain the foundations of probative weight. Further, India's shift from section 65B of the IEA, 1872 to section 63 of the BSA, 2023 is an illustration of both the promise and the limits of reform in legislation. But, an absolute pre-condition to all of this is that the courts should always try to strike a balance between the procurement and resultant usage of digital evidence and the fundamental right of privacy and the constitutional safeguard against self-incrimination as enshrined under article 20 (3) of the Constitution of India. The reliability of digital evidence in the era of cybercrime, hence cannot be secured through a single statute or technology, but by a synthesis of sustained and integrated holistic development of law. At this juncture, it would be best quote Carl Sagan in its entirety –

"Extraordinary claims require extraordinary evidence"

~ Carl Sagan.