Evidence Engineering in IP Litigation

News & Updates • July 14, 2026

First published by Lexology.

Authors: Lakshmidevi Somanath and Kanishka Vaish

I. The Quiet Trend of Strong Evidence Engineering

Anyone who has appeared in a contested IP matter over the last decade will have noticed a distinct shift. The arguments still happen wherein counsel cites doctrine and statute. After this, what actually moves a judge for or against interim relief, once other considerations of law have been satisfied, now sits in the careful preparation of digital evidence. This includes the integrity of hash values, the credibility of forensic capture, and the proper submission of ample electronic material before a court in admissible form. Therefore, Evidence engineering wherever needed, must precede litigation, not follow it.

This litigation phenomenon can be called **evidence engineering**. It is at once three things. There is the collation of evidentiary architecture before any dispute begins. The investigation team makes a note of what gets logged, where, with what cryptographic anchor, and against which neutral source of time. There is the use of technology to submit to the bench confident digital records about the plaintiff or petitioner, that are otherwise by their nature fleeting, scattered, and easily contested. There is also a slow concentration of evidentiary capability in the hands of the litigants, vendors, and platforms equipped to operate at this level. They are effectively aided in this by various AI tools. Seen from the bench, the cases increasingly hinge on the quality of the evidentiary submissions rather than on the elegance of the argument. Therefore, the work of the litigation team towards IP matters today happens much earlier, and in technical layers that do not always make it into the reported judgment.

II. What Evidence Engineering Looks Like in Practice

As an example, we can look at a brand enforcement programme. A proprietor monitoring marketplace does not just observe infringing listings. It captures them through a vendor whose workflow produces, for each capture event, a contemporaneous record. This includes server response headers, full HTML, asset hashes, timestamp evidence drawn from a third-party time authority, and a chain of custody log signed by the operator. Additionally, In Domain name IP dispute matters WHOIS data, layer captures along with independently certified archive retrieval logs, DNS Propagation records need to be captured as operational from time to time. The listing itself may have disappeared by the time the case goes to litigation, but that is irrelevant because the evidence is already gathered. This is because what gets entered into court is the forensically crafted

reconstruction of the listing as it stood at the moment of its capture.

A similar logic is followed by a software illegal use claim. As the plaintiff arrives at the local commissioner stage with imaging specialists, write blockers, and predefined hashing protocols, the defendant's machines are imaged on site, under documented procedure. is the court then looks at the comparison of cryptographic fingerprints across machines preserved in a state the court can trust.

This is what good practice in litigation looks like now. The skilled practitioner understands that much of the case has already been decided by the time pleadings are filed, because the evidence that will determine the outcome was either captured well or captured badly months earlier.

III. Why the Older Evidentiary Model No Longer Travels Far

Classical IP enforcement infrastructure was developed for an environment which was tangible, sluggish, and geographically concentrated. In such an environment, the submission in court would take the form of affidavits of use from witnesses, receipts from trap purchases, and comparisons of products placed on cardboard panels. The said environment has become scarce in regions where the enforcement now takes place. Counterfeit listings switch identity of sellers every week. Pirated streams move from one node to another through reverse proxy. Infringement of software uses compiled binaries. With all this in consideration, the old way becomes rather inadequate.

Digital evidence is able to close many of the gaps in the above evidentiary system. Metadata anchors questions of timing and authorship. This includes EXIF data on listing images, WHOIS histories, DNS records, archive captures preserved with verifiable retrieval logs, etc. Server-side evidence, particularly log files showing deployment histories and access patterns, is more effective than any witness affidavit. Perceptual hashing in copyright disputes, and embedding based clone detection in software disputes, aid the comparative analysis of the court. Platform analytics, including view counts, geotags, and monetisation flows, are able to effectively quantify harm.

Where there is already a compelling case, the failure by the trademark owner to produce WHOIS histories, verifiable archival records, and forensic snapshots of the alleged offending website at an interim hearing is indicative of poor preparation.

IV. The Platform as the Silent Keeper of the Record

In many cases, the critical information is located on the servers of private platforms, accessible to the disputing parties at their discretion alone. Amazon Brand Registry, Meta Rights Manager, YouTube Content ID, Flipkart, and IndiaMart are no longer mere tools of enforcement. They are also the repositories of information about sellers, volume of transactions, listing histories, buyer communication and even information from algorithms. In an ongoing dispute over online

counterfeiting, the information to decide is with the platform.

In live streaming piracy matters, evidence capturing is most compressed evidentiary challenge because of the co-extensiveness of pirated material. A quick timely response and adequate evidence capturing is required. In these cases, recording stream URLs, CDN headers, adaptive bitrate manifests and concurrent geolocations with timestamps is crucial.

Platforms are informal first instance adjudicators. Their internal trust and safety determinations decide whether a dispute reaches a court and on what factual base. If a matter proceeds, the plaintiff's record is composed of whatever data the platform chose to release, in the format it chose to release it. Much depends on the maturity of the platform's processes, the visibility of its rules, and the availability of independent verification. All of thisvaries a great deal across services and jurisdictions.

V. Cryptographic and Algorithmic Proof: Promise and Limits

Blockchain timestamping is increasingly presented as conclusive proof of prior authorship or creation. It is offered through services such as Bernstein, OpenTimestamps, etc. These systems can prove that a particular hash existed at a particular time. They cannot show that the underlying work was original, lawfully created, or attributable to the registrant. A diligent infringer can timestamp a copied work shortly before the original creator notices the appropriation. The probative weight that some forums have begun to attach to such material, may at times sit ahead of what the underlying cryptography actually supports if it is divorced from corroborating context. The Hangzhou Internet Court's 2018 recognised blockchain stored evidence and the procedural rules were later adopted across China's internet courts.

AI generated infringement detection raises related concerns. Perceptual hashing, embedding based similarity scoring, and large model content classification produce outputs. These outputs are probabilistic, threshold dependent, and frequently irreproducible between versions of the same model. The classifiers are typically proprietary. The training data is undisclosed. The false positive rates are not independently audited. A plaintiff submits a report concluding that 84 percent of the defendant's source code is substantially similar to a protected codebase. Then the question that really matters is what substantially similar means within that specific embedding model, on that corpus, at that confidence threshold.

Therefore, technologically supported and generated evidence carries an aura of objectivity that older documentary evidence did not. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal And Ors.*,, the Hon'ble Supreme Court examines the Evidence Act as it deals with the authentication of electronic records as records and held that certificate under Section 65B is mandatory and cannot be substituted by oral testimony.

VI. India's Procedural Improvisation

India has built a technologically intensive procedural environment through judicial innovation and statutory updating. Section 65B of The Indian Evidence Act, 1872, provides the foundational gateway for electronic records, without Section 65B certificate any electronic evidence is inadmissible. The Anton Piller styled appointment of commissioners has developed from a routine practice in India's intellectual property practice into forensic activities that have been formalized. The commissioners can now receive assistance from experts in imaging, write blockers, hash verification and even instructions to mirror servers and cloud synchronization. The Commercial Division of the High Court of Delhi has developed the role of the commissioner to include forensic preservation of IT infrastructure.

In *UTV Software Communication Ltd. v. 1337x.to*, the practical impossibility of chasing every variation of a piracy operation through separate proceedings was looked at. To tackle the hydra-headed aspect of the rogue website taking different forms such as mirror sites, redirects, and alphanumeric sites, the Court allowed the plaintiffs to bring those successor websites under the ambit of Order I Rule 10 of the Code of Civil Procedure, 1908, with a referral to the Joint Registrar for extending the orders in respect of blocking. Later developments including the adoption of "dynamic plus" injunctions, and the subsequent extension in Star India Pvt Ltd v IPTV Smarter Pro and Ors to include what some Courts have termed "superlative" injunctions irrespective of the means of distribution of the offending material, indicate that the procedure adopted amounts to evidence engineering within the very confines of the Court itself.

The transition from considering electronic records as only supplementary proof to considering them as the main source of determining infringement in the digital world. Decisions made by the Supreme Court in *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* established the foundation for the admissibility of electronic records, the Delhi High Court's IP jurisprudence further evolved on the authenticity, attribution, and probative value of such evidence. In *Excitel Private Limited v. Registrar of Trade Marks*, the Court rejected the argument that website printouts and internet extracts are inherently unreliable, holding that online material may be a valid evidence of when properly authenticated. Similarly, in *Christian Louboutin SAS v. Nakul Bajaj* and *Kent RO Systems Ltd. v. Amit Kotak*, the Court relied extensively upon website screenshots, online listings, and digital representations to assess the manner in which products were marketed and perceived by consumers.

For instance, in cases relating to software piracy like the case of *Microsoft Corporation v. Yogesh Papat*, one can see how courts give a lot of evidential importance to forensic analysis of hard drives and software inventories. Conversely, courts have shown equal reluctance to act upon inadequately proved electronic records. In the Division Bench decision in *Super Cassettes Industries Ltd. v. MySpace Inc.* the allegations of online infringement, not supported by identification of specific URLs

or digital files, are insufficient to sustain a claim of infringement.These combined together show that the question in intellectual property dispute today is not about the existence of electronic evidence but whether the party presenting the evidence can prove a chain of digital evidence that shows its origin, authenticity, and accuracy. Indian courts have been using electronic evidence as the main factual basis for resolving intellectual property disputes arising from the activities performed on the internet. This can be seen from the case *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy* where the Court took into account website accessibility, internet presence, and online targeting to decide if the defendants' internet activities created a territorial jurisdiction. Likewise, in the case of *Tata Sons Ltd. vs. Greenpeace International*, the court took into account several instances of website publications and campaign material on the web as primary proof for determining the effect of the impugned use.

In the context of online copyright infringement, courts have routinely relied upon screenshots, website captures, domain registration records, and investigator-generated digital evidence. For instance, in *Disney Enterprises Inc. v. Kimcartoon.to*, the Court relied substantially on website screenshots, domain information, online monitoring reports, and investigator evidence to establish the operation of infringing rogue websites. Similarily, in *Universal City Studios LLC v. Fzmovies.net*, the Court issued an injunction based on captures from websites, webpages for streaming, evidence of copyright infringement through online piracy, and documentation regarding the domains. In *Warner Bros. Entertainment Ltd. v. Uwatchfree*, the Delhi High Court was guided by the following materials from the websites: evidence from the websites, links for the streaming, availability of the copyrighted content on the internet, and digital surveillance materials. Together, these rulings illustrate the extent to which the court is willing to consider electronic documents not as supportive evidence, but as substantive evidence that can prove infringement, business activity, and the nature of the digital actors involved, on condition that the document is authenticated to the accused individual

The significance of digital documents in the criminal process was established in two significant cases. In State*(NCT of Delhi) v. Navjot Sandhu*, the "Parliament Attack Case," the Court held that call-detail records secondary evidence could be admitted under Sections 63 and 65 of the Indian Evidence Act, 1872 without formal Section 65B certification, acknowledging the practical difficulty of producing entire computer systems in court. This flexible approach was reinforced in *Mohd. Ajmal Amir Kasab v. State of Maharashtra*, where the Court held that internet transaction transcripts were important in proving the accused guilty in the 26/11 terror attacks. Beyond admissibility, this case established a very crucial overview of how courts look at electronic evidence, that is when a prosecution possesses best evidence such as CCTV footage or any other evidence which are conclusive proofs and withholds it, courts is at liberty to draw an adverse inference under Section 114(g) of The Indian Evidence Act,1872, treating non-production of evidence as evidence tampering. Together, these cases established that electronic evidence is not merely supplementary but central to criminal prosecution, while simultaneously imposing an affirmative duty on parties to produce available digital evidence or face adverse consequences in judicial proceedings.

Acceptance Electronic Evidence Beyond Mere Section 65B Certificate of The Indian Evidence Act,1872

In *State (N.C.T. of Delhi) v. Navjot Sandhu @ Afsan Guru*, The Court held that electronic records could be proved through traditional modes of evidence under Sections 63 and 65 of The Indian Evidence Act, 1872, even in the absence of a certificate under Section 65B(4). Also the Court put forth that what is to be looked at in the case of admissibility of electronic evidence is the case to case basis which includes the evidence's reliability, it's source and how it was produced.

Indian courts have time and again stressed that for the admissibility of electronic records what is important is compliance with Section 65B of The Indian Evidence Act of 1872 but the which is that of authenticity, reliability, source and relevance to the issue in dispute is what the courts look at. Also it is brought out in many a judgment that although the Section 65B certificate is obtained4 it is the substance and probative value of the electronic evidence which the courts evaluate which sometimes may not be in favor of the said certificate.

Claims Faltered Due To Inadequately Proved Electronic Evidence

It has been found time and again by the Indian courts that the electronic evidence should first fulfill the criteria for being admissible and authentic as per the statutory provisions. Otherwise, the electronic evidence might lose its relevance, and consequently, it would weaken or even fail the case of one party.

In *Sonu @ Amar v. State of Haryana*, the Supreme Court dealt with Call Detail Records (CDR) that had been admitted into evidence without a Section 65B certificate. While reiterating that electronic records are ordinarily not admissible without the requisite certificate, the Court held that objections concerning the mode/method of proof must be raised at the time the evidence is tendered. Since no objection had been taken before the trial court, the appellants were not allowed from challenging the admissibility of the CDRs at the appellate stage. The judgment illustrates that although inadequately proved electronic evidence may be vulnerable to challenge, such objections can be waived if not raised at the appropriate stage.

A diverse approach was adopted in *Silambarasan v. State represented by Inspector of Police*, where the prosecution relied upon CDRs to establish the nexus between the accused. The lower court used the CDRs on account of the absence of any objection in this regard at the time of their production. The higher court, in turn, citing the ruling made in the case of Arjun Panditrao Khotkar as well as other judgements from the Supreme Court of India, stated that the electronic documents lacking a proper certificate under Section 65B could not be used in court. As a result, the evidentiary value of the CDRs became nullified, and one of the main grounds for the prosecution was discredited.

It must also be noted that the above-mentioned jurisprudence is based on the judgement made by

the Supreme Court of India in the case of *R.V.E. Venkatachala Gounder v. Arulmigu Viswesaraswami & V.P. Temple*, wherein the Supreme Court held that objections to the admissibility or mode of proof of evidence should ordinarily be raised at the time the document is tendered. This principle has subsequently been applied in several electronic evidence cases to determine whether challenges to admissibility have been waived.

Similarly, in *Directorate of Revenue Intelligence v. Suresh Kumar & Company Impex*, the Court observed that the necessity and applicability of a Section 65B certificate must be examined in light of the facts and circumstances of the particular case, while been guided by the principles laid down in *Arjun Panditrao Khotkar case*. Also in that decision it is brought to light that courts do not put forth formal compliance with Section 65B as sufficient but also look into the overall reliability and provenance of the electronic record.

Evidence that relies heavily on electronic evidence could fail due to the fact that the electronic evidence does not have the proper authentication or certification under the statute required for it. Although the rules of admissibility still apply to Section 65B, the courts are now considering issues beyond mere admissibility when dealing with electronic evidence.

VII. A Comparative Look Outward

This is an international trend. Singapore has been able to place itself on the technological side through its technology-specialized courts and the Singapore International Commercial Court. The United Kingdom considers the competence of electronic disclosure to be a minimum requirement, and this is achieved using Practice Direction (PD) 57AD. The internet courts in Hangzhou, Beijing, and Guangzhou have managed to develop a system where evidence in the form of blockchain and algorithmic evidence is integrated directly into the procedural rules. The internet courts in Hangzhou, Beijing, and Guangzhou have built a framework that pulls blockchain stored and algorithmically derived evidence directly into procedural rules. The United States has retained rigorous adversarial testing of digital evidence under the Federal Rules of Civil Procedure. The other regulations are the ESI protocols developed through the Sedona Conference, with Daubert style scrutiny applied to algorithmic methods and preservation and production, ultimately imposing sanctions. Furthermore, under which federal trial judges act as gatekeepers screening expert and scientific evidence for reliability before it reaches the factfinder.

Procedural sophistication has become a competitive attribute of jurisdictions in the global IP marketplace. Forum selection is not based merely on substantive standards. It also depends on a forum's evidentiary culture, i.e. its willingness to accept platform derived datasets without elaborate foundation, its capacity to scrutinise algorithmic methods, its speed in preserving digital material, and the robustness of its confidentiality regimes. India's commercial divisions are competitive on these metrics.

VIII. Possible Directions

Rules related to probabilistic and algorithmically derived evidence would help. , Rules could be formalised under the Information Technology Act for addressing disclosure of methodology, error rates, and reproducibility for evidence offered through automated systems. Evidence engineering is now a precondition of effective enforcement. Similarly the cost of enforcement has risen too. Whether this is best understood as a problem of access to justice, of competitive industrial policy, or simply of practice catching up to technology, will depend on where one stands. Mechanisms can be made to extend forensic capability to less resourced litigants, perhaps through empanelled neutral experts. The future of IP enforcement is a more practical call. This is to take the procedural and technological infrastructure of evidence as seriously as the legal community has long taken the substantive law that this infrastructure now carries.

To view all formatting for this article (eg, tables, footnotes), please access the original here.

KEY CONTACT

Lakshmidevi Somanath

Partner

View Bio of Lakshmidevi Somanath