

Towards a Tech-Savvy Judiciary: A Comparative Study of Evidentiary Flexibility in India, the UK, US, Canada, and Singapore

Himanshu Thakran

Research scholar, Department of Law, Gurugram University Gurugram

Abstract

The 21st century has witnessed a profound digital transformation, fundamentally altering the way individuals communicate, transact, and store information. With the widespread proliferation of devices such as smartphones, laptops, and cloud-based platforms, electronic evidence comprising emails, digital images, chat logs, GPS data, and multimedia files has become indispensable in both civil and criminal litigation. This paper examines the evolving legal treatment of electronic evidence in India, contextualized through a comparative analysis of five common law jurisdictions: the United States, the United Kingdom, Canada, Singapore, and India.

Through this comparative lens, the study identifies key strengths and limitations in India's current evidentiary framework, particularly in light of the Bharatiya Sakshya Adhiniyam, 2023. It explores issues surrounding the authenticity, admissibility, integrity, and chain of custody of digital evidence, while assessing procedural and technological safeguards necessary for fair adjudication. Drawing from international best practices, the paper offers targeted recommendations to enhance India's approach, ensuring it remains both technologically relevant and jurisprudentially sound. Ultimately, the study underscores the need for a flexible, secure, and harmonized evidentiary regime that can uphold justice in a digitally interconnected world.

Keywords

Electronic Evidence, Digital Admissibility, Comparative Legal Analysis, Evidentiary Integrity, Legal Reforms, Tech-Driven Justice.

Introduction

The 21st century has brought a major technology boom that has changed lives not only in India but across the world. Computers, once used mainly by big organizations, are now available to almost everyone in different forms, like laptops, smartphones, and tablets. This digital revolution has created a virtual world called cyberspace, where the internet connects people, businesses, and governments globally. However, this connected world also gives opportunities to both law-abiding citizens and criminals to access information using advanced technology.

As more people rely on digital devices for communication, online shopping, and storing information, the way evidence is used in courts has changed. Electronic evidence, or e-evidence, is now crucial in both civil and criminal cases in India. This includes things like emails, digital photos, ATM records, digital documents, chat histories, GPS data, and audio or video files. These types of evidence are unique because they are easy to copy, hard to destroy completely, easily changed, and often more detailed than traditional evidence. These features create both opportunities and challenges for the legal system.

To understand how electronic evidence is handled, this research compares the laws in different countries: the United Kingdom, the United States, Canada, Singapore, and India. Comparing legal systems helps identify what works well and what can be improved. This study focuses on specific rules about electronic evidence rather than entire legal systems. Electronic evidence is defined as any data created, stored, or sent through devices like computers or smartphones that is relevant to solving a legal dispute. This definition includes various devices and ensures the evidence is useful for court decisions.

This research is particularly relevant in today's world, where digital devices have become indispensable to daily life. From facilitating local and global communication to enabling e-commerce and digital record-keeping, technology has transformed how individuals and organizations operate. However, this increasing dependence on digital platforms also amplifies risks, including cybercrimes, data breaches, and evidence manipulation, which pose significant challenges to legal systems. By analysing the experiences of other jurisdictions, this study aims to offer actionable recommendations for strengthening India's legal framework for electronic evidence. These recommendations will focus on improving the admissibility standards, ensuring the integrity of e-evidence, and fostering greater alignment with global best practices.

Ultimately, this research seeks to contribute to the ongoing discourse on the evolution of IT laws in India and the global harmonization of standards for electronic evidence. By providing a comprehensive comparative analysis, the study aims to equip policymakers, legal practitioners, and scholars with valuable insights into how India can navigate the complexities of the digital era while upholding the principles of justice, fairness, and equity. Through this exploration, the research underscores the importance of adapting legal systems to the realities of a technology-driven world, ensuring that the administration of justice remains robust, reliable, and responsive to the needs of a rapidly changing society

Comparative analysis of electronic evidence frameworks

United Kingdom

Electronic evidence is governed by distinct legal principles in comparison to traditional documentary evidence, particularly under the UK's Civil Evidence Act, 1968 and the Police and Criminal Evidence Act, 1984. Under these statutes, computer-generated documents are admissible only if their authenticity is proven by fulfilling specific criteria, such as regular data input and functioning of the computer during the relevant period, and that the information recorded accurately reflects what was input into the system. A certificate signed by the responsible operator is required to establish the reliability of such records. Additionally, the court must consider the timing of the data recording and any potential motive to manipulate facts when evaluating the probative value of such evidence. Notice must also be given to the opposing party prior to relying on such evidence in court¹.

The Police and Criminal Evidence Act, 1984 similarly allows the admissibility of electronic evidence in criminal proceedings, contingent upon the absence of reasonable grounds for questioning the accuracy of the data due to computer misuse or malfunction². However, these provisions have led to considerable judicial uncertainty due to their technical complexity. For

¹ Civil Evidence Act, 1968, s. 5; Police and Criminal Evidence Act, 1984, s. 69.

example, in *R v. Maqsd Ali*, tape recordings were admitted based on analogies drawn with photographs and other visual aids, provided their accuracy could be verified. In *R v. Spiby*, telephone call logging printouts were treated as real evidence in the absence of proof of malfunction. Similarly, in *Camden LBC v. Hobson*, the court differentiated between mechanically generated data and human input processed by a computer, admitting the former as real evidence³.

In *Castle v. Cross*, breath test machine printouts were admitted as direct evidence since the information was machine-generated. The ruling in *R v. Shephard* clarified that computer records can be accepted as long as the system's reliability and proper use can be established. This approach has been echoed in recent cases such as *Intercity Telecom Ltd v. Sanjay Solanki*, where USB and electronic device contents were admitted as evidence, and *Atkins v. The Lord Chancellor*, which allowed CCTV footage to be used in a criminal proceeding³.

Furthermore, *Glenn Whittle v. The Commissioner* reinforced that computer-generated documents, including financial and transport records, are admissible if they are stored and retrieved properly. Under the Youth Justice and Criminal Evidence Act, 1999, video recordings from vulnerable witnesses are also accepted, provided they are appropriately verified during trial.

Electronic evidence generally falls into two categories: information stored by computers upon human input, and data autonomously generated by computers or in coordination with machines. Section 65B of the Indian Evidence Act attempts to address such evidence but has been critiqued as an outdated reproduction of the UK's repealed Section 5 of the Civil Evidence Act, 1968. The UK repealed this provision in 1995 following the Law Commission's recommendation, citing advances in technology and redundancy in maintaining a separate legal framework for computer records. This highlights the need for a similar legislative update in India to tackle practical challenges posed by the current framework⁴.

E- evidence in the us

The rise of electronic evidence has not necessitated a significant overhaul of the Federal Rules of Evidence (FRE), as these traditional rules can be applied to the analysis of such evidence. It is important to recognize that the electronic nature of evidence does not alter the fundamental principles of its admissibility; rather, it is treated similarly to non-electronic evidence in many respects (Moore, 2010)⁵. While challenges related to authenticity and foundation may arise, the framework established by the FRE remains robust for addressing the admissibility of electronic data (Phillips, 2010)⁶.

In the United States, electronic evidence is categorized into two types: background and foreground evidence (Grimm & Joseph, 2017)⁷. Background evidence refers to electronically stored data generated during regular business activities, such as network logs, authentication records, backups, and application security logs. Foreground evidence, on the other hand, is created as a result of specific activities or interactions related to the investigation, including

communications via email, instant messaging, and real-time monitoring systems (Grimm & Brady, 2018)⁸.

In the landmark case *United States v. Liebert* (1975), the court set forth criteria for admitting computer-generated evidence in a criminal trial. The prosecution must prove that the information obtained is accurate and has not been tampered with, while the defense is granted an opportunity to challenge the accuracy of the data (Grimm & Joseph, 2017). The FRE provides two methods for authenticating electronic records: the traditional method under Rule 901 or through self-authentication as per Rule 902. Rule 901 establishes that evidence must be authenticated by sufficient proof to support a finding that the evidence is what it claims to be, with specific emphasis on the reliability of the process or system that generated the evidence (Federal Rules of Evidence, 1975).

Moreover, electronic records can be authenticated using distinct methods, such as expert testimony or comparison with authenticated examples (Federal Rules of Evidence, 1975). In *Lorraine v. Markel American Insurance Co.* (2007), the court ruled that electronic evidence must be relevant, authentic, and not subject to exclusion under hearsay rules. The court also emphasized the need for electronic evidence to be presented in its original form or as a reliable duplicate, in line with the best evidence rule (Moore, 2010).

The acceptance of electronic business records is further clarified by Rule 803(6) of the FRE, which permits the admission of business records made in the regular course of business as an exception to the hearsay rule. This provision applies to electronic records as well, provided that they are made contemporaneously by someone with knowledge and are stored according to the business's regular practices (Grimm & Brady, 2018).

The 2017 amendments to Rule 902 introduced sub-rules (13) and (14), which allow for the self-authentication of electronic records, particularly those generated by automated processes or systems. While these amendments streamline the process, Rule 901 continues to apply to all forms of evidence, ensuring that traditional authentication methods remain applicable to electronic records (Grimm & Joseph, 2017).

In conclusion, the legal framework in the United States has evolved to accommodate the growing use of electronic evidence without abandoning traditional principles of admissibility. By incorporating provisions for the authentication and acceptance of digital records, U.S. courts have adapted to technological advancements while maintaining the integrity of the evidentiary process.

Status in singapore

With the rise of digital technology, document creation and storage have dramatically transformed. A 2004 study found that over 90% of documents produced in many organizations today originate digitally, with 70% never being printed⁹. This shift has led to an influx of digital evidence types—such as metadata, emails, and multimedia—which were previously unimaginable in legal proceedings¹⁰. Recognizing the inadequacies of traditional evidentiary

rules, Canada introduced the Uniform Electronic Evidence Act in 1998. Singapore soon followed, amending its Evidence Act in 1996 to avoid similar pitfalls¹¹.

Admissibility of Computer Output Pre-Amendment

Before 2012, Sections 35 and 36 of the Evidence Act 1981 governed the admissibility of what was termed “computer output.” These provisions applied to all forms of outputs from standalone systems, networked systems, and multimedia content. Section 35(1) specified that computer output was admissible if it was relevant and fell under any one of the following:

- Where both parties agreed that neither the authenticity nor the accuracy of the computer output would be disputed;
- Where the output was produced through an “approved process”;
- Where the proponent of the evidence proved that it was generated by a reliable and properly functioning system.

However, these requirements often proved impractical. In adversarial proceedings, the first condition was rarely fulfilled. The second—requiring audit and certification by a Ministry-approved agency—was often time-consuming and costly¹². The third condition required supporting affidavits and certificates from system operators confirming reliability, which was not always feasible. Even though courts later relaxed this requirement to allow any person familiar with the system to testify¹³, challenges persisted due to the complexity of assessing digital systems.

Admissibility Post-Amendment

The Evidence (Amendment) Act, 2012 repealed Sections 35 and 36 and replaced them with a new framework under Section 116A. This introduced three rebuttable presumptions:

1. Accuracy Presumption – If the device/process usually produces electronic records reliably, the court presumes it did so.
2. Authenticity Presumption (Third Party) – If a record was created by someone not involved in the proceedings, it is presumed authentic.
3. Authenticity Presumption (Adverse Party) – If a record was created by an adverse party and used against them, it is presumed authentic.

These were drawn from Canada’s Uniform Electronic Evidence Act, 1998 and Australia’s Evidence Act, 1995³. The amendments also modernized definitions. “Computer” and “computer output” were replaced with broader definitions like “document” and “electronic record,” covering digital images, audio, video, and stored/transmitted data¹⁴.

Judicial Precedents

In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, the court admitted over 2,000 third-party emails as evidence of the defendant’s knowledge of copyright violations¹⁵.

In *McKeown v. DPP*, the House of Lords ruled that malfunctioning equipment does not render evidence inadmissible if the malfunction does not affect the accuracy of the output. Here, a faulty Intoximeter clock did not impact the breathalyzer reading, which was held admissible¹⁶.

Position in Canada

In 1918, Canadian commissioners convened a meeting in Montreal to discuss the need for uniform laws across the country. This led to the recommendation of a model law for Uniform Electronic Evidence in September 1998, which was later reflected in amendments to the Canada Evidence Act, 1985. The core idea was that all documents, including electronic ones, must be authenticated before being admitted as evidence. Authentication refers to providing sufficient evidence to establish that the documents are indeed what they purport to be, and that they are relevant to the case at hand.¹⁷

Authentication of Electronic Documents

For any party wishing to admit an electronic document into evidence, it is their responsibility to prove its authenticity. This means presenting evidence that can establish that the document is what it is claimed to be¹⁸. The Ontario Evidence Act similarly imposes this obligation on the party attempting to introduce electronic records, specifying that they must prove the authenticity of the record by presenting suitable supporting evidence.³

To effectively introduce electronic evidence, it is advisable for a party to maintain detailed logs documenting the electronic file's history, which should include the following information:

1. Identification of each piece of evidence.
2. Details regarding who possessed the evidence, along with the date, time, and location.
3. A description of actions taken while the party had possession of the evidence.
4. Details of the programs and procedures used to move or copy the data.
5. Records of any changes in location or possession of the evidence.¹⁹

Best Evidence Rule and Electronic Documents-

Section 31.2(1) of the Canada Evidence Act states that the best evidence rule can be satisfied with proof of the integrity of the system in which the electronic document was recorded or stored. Alternatively, an evidentiary presumption under Section 31.4 may also apply. Printouts, under Section 31.2(2), are accepted as the best evidence if they have been consistently relied upon in the usual course of business.²⁰

Further, Section 31.3 specifies how the integrity of an electronic documents system should be proven. This includes demonstrating that the system was functioning correctly or that any malfunction did not affect the document's integrity. Additionally, it is acceptable if the electronic document was created or stored by a third party unrelated to the party seeking to introduce it.²¹

Standards and Practices for Electronic Evidence

Section 31.5 allows for the presentation of evidence regarding any relevant standard, procedure, or practice used in recording or storing electronic documents, which may affect the admissibility of the evidence. The specific standards depend on the type of business or operation involved and the nature of the document.²²

Additionally, Section 31.6 allows these matters to be established via affidavit. Cross-examination of an affidavit's deponent is allowed if the deponent is either an adverse party or under the control of one.

Judicial Interpretation and Application-

Although Section 31.3 and Section 31.6(1) of the Canada Evidence Act seem to suggest a similarity to Section 65B of India's Evidence Act, a key distinction lies in how Canadian law handles documents stored by adverse parties. For example, Section 31.3(b) allows for documents stored by an opposing party to be introduced, provided certain conditions are met. In contrast, Section 31.3(c) extends this to documents created or stored by a third party under neutral conditions.

In *R. v. Bishop*, the court referred to the new rules as a "mini-code," suggesting that they provide a comprehensive approach to electronic evidence, prevailing over other legal provisions in some cases.²³ However, in *R. v. Ganes*, the court ruled that pre-existing rules regarding professional reports for licensing and signatures outweighed the newer provisions for authentication and best evidence, showing the limitations of the new rules.²⁴

In *R. v. Sanghi*, the court accepted that a computer-generated printout was considered an original record if processed in the regular course of business.²⁵ However, in *Shah v. R.*, the defendant argued against the admissibility of printouts in different forms, but the court concluded that the electronically stored data was the original record, regardless of the form it was presented in.²⁶

Specific Cases Involving Electronic Evidence

In *Symanski v. R.*, it was determined that the provisions of Sections 29 and 30 of the Canada Evidence Act are separate, and a document that might be inadmissible under one section could still be accepted under the other. This flexibility allows for the admissibility of computer-generated documents in various circumstances, such as financial records or business documents.²⁷

The case *McMillan v. R.* highlighted the distinction between the two sections, noting that while Section 30 does not establish the probative value of records, it is up to the judge to determine their weight based on the circumstances of each case.²⁸

In *McCulloch v. R.*, the court refused to accept telephone call records as evidence because they were not made in the ordinary course of business but rather as part of an extraordinary procedure to produce evidence. This case emphasized that the circumstances under which evidence is generated play a crucial role in determining its admissibility.²⁹

Recent Reforms and Proposals

To address the uncertainties surrounding electronic evidence under the Canada Evidence Act, the Uniform Law Conference of Canada has recommended amendments to clarify these issues. Among the proposed changes is a more comprehensive definition of “record” that would apply to all documentary evidence and the introduction of clearer standards for determining the status of computer-generated records, both in terms of their authenticity and their admissibility as evidence.

Position in india

Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

India has taken a major step toward modernizing its legal system with the introduction of the Bharatiya Sakshya Adhiniyam, 2023 (BSA). This new law replaces the outdated Indian Evidence Act, 1872, and brings with it significant reforms—especially in how electronic evidence is treated in court.

One of the most important changes in the BSA is how it deals with digital and electronic records. The old law, particularly Section 65B, was often criticized for being unclear and difficult to apply. Courts struggled with interpreting its requirements, which led to inconsistent rulings. The BSA addresses this issue with a fresh and detailed approach through Sections 61 to 63, making the law more suitable for the digital age.

Equal Status for Electronic Evidence

Section 61 of the BSA is a game-changer. It clearly states that electronic and digital records are to be treated just like traditional paper documents. The law says that no one can reject a document just because it is in an electronic or digital format³⁰. If certain conditions under Section 63 are met, these digital records have the same legal value as handwritten or printed ones¹. This is an important recognition of the role technology plays in modern life, from emails and mobile messages to cloud-based files and server logs.

Clear Process for Proving Digital Records

Section 62 simplifies how the contents of electronic records can be proven. It says that electronic records must be proved according to the rules in Section 63³¹. This approach avoids confusion by making it clear that all the conditions for admissibility are located in one place, unlike the older Evidence Act where Section 65B often clashed with other provisions.

Requirements for Admitting Electronic Evidence

Section 63 is the heart of the BSA’s electronic evidence framework. It describes the conditions under which electronic records can be admitted in court. It starts by explaining what counts as a “computer output.” This includes any data printed on paper, saved on magnetic or optical media (like CDs or hard drives), stored in chips, or kept in any electronic format. As long as the data came from a computer or communication device used during regular activities, it can be considered valid evidence³².

Section 63(2) outlines four key conditions that must all be met for the electronic evidence to be accepted:

1. Regular Use – The computer or device must be used regularly to store or process the kind of data now being submitted as evidence.
2. Routine Data Input – The data must have been entered into the device during normal business or personal activities.
3. Proper Functioning – The device must have been working properly during the relevant time, or any problem must not have seriously affected the accuracy of the data.
4. Accurate Output – The digital output (the record being submitted) must be a true and accurate copy or version of the original data³³.

These rules are similar to what was previously required under the old Section 65B, but the BSA presents them in a much clearer and more modern way. It also introduces updated terms like “communication device” and “electronic form,” showing the law’s intent to include newer technologies like smartphones, emails, and cloud platforms.

Handling Complex Digital Systems

One of the most forward-thinking parts of the new law is Section 63(3). It recognizes that digital information is often stored across multiple systems, not just on one computer. For example, cloud-based data may pass through different servers in different locations. This section says that all devices involved in storing or processing such data should be treated as one single system³⁴. This makes it easier to admit evidence from complex technological systems, which are now common in businesses and personal use.

Hence, The Bharatiya Sakshya Adhiniyam, 2023, marks a significant advancement in how India handles digital evidence. By giving electronic records equal standing with paper documents and clearly laying out the rules for their admissibility, the BSA makes the legal process more efficient, modern, and fair. These reforms bring Indian law closer to current global standards and address the growing need for clear, technology-friendly evidence rules in the digital age.

Analysis and comparison of india with other countries

India’s Bharatiya Sakshya Adhiniyam, 2023 (BSA) modernizes the country’s evidentiary framework by giving digital records equal legal standing with traditional documents. This legislative shift places India in alignment with global trends, where jurisdictions like the USA, UK, Canada, and Singapore have similarly acknowledged the importance of electronic evidence. However, while the principles of authenticity and reliability remain central across these systems, the Indian approach retains certain formalistic traits that distinguish it from more flexible international practices.

Key Findings and Comparative Assessment

Jurisdiction	Admissibility Standard	Authentication Method			Judicial Discretion
UK	Reliability-based	Certification (formerly)			Moderate
US	Relevance authenticity	&	Rule 901/902, certification	self-	High

³³ Bharatiya Sakshya Adhiniyam, 2023, Section 63 (2)

³⁴ Bharatiya Sakshya Adhiniyam, 2023, Section 63 (3)

Jurisdiction	Admissibility Standard	Authentication Method	Judicial Discretion
Singapore	Rebuttable presumptions	System reliability proofs	Moderate-High
Canada	Integrity-focused	Logs, affidavits	High
India (BSA)	Structured statutory tests	Mandatory certification	Limited

Critical Observations:

- India's *BSA* aligns with global trends but retains procedural rigidity.
- The US and Canada prioritize judicial discretion, while Singapore uses presumptions to streamline admissibility.
- India's certification mandate may hinder efficiency in cloud-based and complex digital evidence cases.

In terms of admissibility, BSA Section 61 mirrors the inclusive approach of the USA's Federal Rules of Evidence, which treat electronic documents as no different from physical records. Similarly, Canada's Evidence Act and Singapore's amended Evidence Act recognize electronic records as valid documents, though often with more flexible criteria for their admission. India's position is progressive in recognizing digital evidence formally but still demands compliance with structured statutory tests under Section 63, a contrast to the US system, which allows broader judicial discretion and less rigid procedural prerequisites.

A significant point of divergence is the requirement for certification. Under Section 63(4) of the BSA, India mandates a certificate from a person in charge or an expert, describing the system used and affirming that all foundational conditions have been met. This resembles Malaysia's and Singapore's earlier models but stands in contrast with the USA, where certification is optional under Rules 902(13) and (14), and authentication may be achieved by other means. Canada too does not strictly require certification, offering courts a range of authentication tools. This shows that while India ensures strong evidentiary control, it may also face practical challenges, especially in cases involving cloud computing or outsourced IT systems.

Unlike Singapore and Canada, which apply presumptions of reliability once system integrity is shown, India's law places the full burden on the party tendering the evidence. While this ensures cautious scrutiny, it may delay proceedings where the evidence is clearly authentic but lacks formal documentation. Moreover, judicial discretion in India is more limited than in the USA, where courts can assess electronic evidence based on relevance and context without insisting on procedural formalities.

Lastly, while India's BSA provides detailed guidance on electronic records, its terminology is not harmonized with the Information Technology Act, 2000, unlike the integrated definitional approach seen in Canada and the US. This could lead to interpretive uncertainties in complex cases involving cybersecurity or data governance

Conclusion

In conclusion, the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), signals a progressive and much-needed evolution in India's evidentiary framework, aiming to bring the country's legal processes in line with the technological and societal shifts of the 21st century. It replaces colonial-era provisions with principles better attuned to contemporary realities, particularly concerning the admissibility and reliability of electronic and digital evidence. This legislative reform reflects the Indian state's recognition of the growing relevance of technology in both civil and criminal adjudication.

However, despite its forward-looking provisions, the BSA remains relatively conservative in structure when juxtaposed with the evidence laws of other advanced common law jurisdictions. It continues to retain a largely rule-based and formalistic approach, which, while offering clarity, can limit judicial discretion and adaptability. This rigidity, though rooted in a desire for procedural uniformity and fairness, may in practice hinder the efficient resolution of disputes in complex, tech-driven cases.

A comparative analysis reveals that countries such as the United States emphasize judicial flexibility in the assessment of evidence, allowing courts greater latitude in determining admissibility based on relevance and probative value, particularly through the Federal Rules of Evidence. The Canadian model incorporates principles of proportionality and balancing of interests, ensuring that evidentiary procedures do not overshadow substantive justice. Meanwhile, Singapore's judiciary has embraced technological pragmatism, streamlining evidentiary rules to encourage swift adjudication without compromising on core rights, as reflected in its Evidence Act and related digital litigation practices.

Drawing lessons from these jurisdictions, India could benefit from incorporating a more context-sensitive and discretionary approach into its evidentiary system. This would entail empowering courts with greater interpretive leeway, especially in evaluating digital evidence, while still upholding the constitutional values of fairness, due process, and the right to a fair trial. Moreover, the integration of guiding principles on proportionality, minimal procedural burden, and technological neutrality could ensure that evidence law remains robust yet responsive to the evolving needs of justice.

Therefore, while the BSA is a commendable reform, it should not be viewed as the terminus of evidentiary modernization. Instead, it must serve as a foundational framework capable of future expansion and judicial innovation. A dynamic and comparative approach, guided by both domestic imperatives and international best practices, will be essential to developing an evidence law regime that is not only modern in form but also transformative in substance.