# DRONE-GENERATED DIGITAL EVIDENCE IN INDIA: BRIDGING THE GAP BETWEEN THE DGCA DRONE RULES, 2021 AND THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Mridula Dharshini M, SASTRA Deemed University, Thanjavur

**ABSTRACT**

In India, drones have quickly transitioned from the military and hobbyist use to everyday civilian, commercial and law-enforcement applications — from crop surveys and infrastructure inspection to encroachment monitoring and criminal investigation. As their footage increasingly features in courtrooms, a key legal question remains mostly unaddressed: Is India's current legal framework really equipped to deal with drone-generated evidence reliably? This paper argues that it does not. The Indian Drone Rules, 2021, made under the Aircraft Act, 1934, are almost exclusively concerned with airspace management, registration and operational compliance, and do not cover at all evidentiary aspects including data preservation, tamper-proofing and authentication.

The Bharatiya Sakshya Adhiniyam, 2023, in contrast, which modernises the treatment of electronic records under Section 63, was drafted keeping in mind conventional digital evidence such as call records, emails and CCTV footage and does not take into account the distinctive features of drone-captured data, which include geospatial metadata, flight-log correlation, live-streamed footage and cloud-based storage across multiple jurisdictions.

This paper doctrinally discusses the real-world implications of this divide such as inconsistent treatment by the judiciary, and the reduced reliability of drone footage in criminal and civil proceedings. This paper attempts to explore possible legislative and regulatory solutions to fill this void with particular reference to the need for clarificatory guidance under the Bharatiya Sakshya Adhiniyam and drone-specific chain-of-custody protocols.

**Keywords:** drone forensics; electronic evidence; Bharatiya Sakshya Adhiniyam, 2023; Drone Rules, 2021; Digital Sky Platform; Section 63; chain of custody

# INTRODUCTION

## I. Background of study

Unmanned aerial systems which is also termed as "drones" (defined under *Under Rule 3(i) of the Drone Rules, 2021*) have moved from novelty instrument of aerial photography to standard instruments of State administration, commercial enterprise and criminal investigation and civil litigation in India. Since drones are used more nowadays their footages are more often used as evidence in the courtrooms in criminal trials, property disputes, and encroachment cases.

The regulation that governs this technology in India are *Drone Rules, 2021 (G.S.R. 589(E), notified 25 August 2021*), administered by the Directorate General of Civil Aviation (DGCA) through the Digital Sky Platform and *The Bharatiya Sakshya Adhiniyam, 2023 (BSA),* which came into force on 1 July 2024 in place of the Indian Evidence Act, 1872.The Drone rules classifies drones by weight (Nano, Micro, Small, Medium and Large categories[1]), mandates registration, issues a Unique Identification Number (UIN) , states about Remote Pilot Certification and operationalise the "No Permission – No Take-off" (NPNT) protocol. The *Bharatiya Sakshya Adhiniyam, 2023 (BSA)* governs electronic evidence. *Section 63 of the BSA* states about admissibility of electronic records in court of law[2]. Electronic records include CCTV footage, emails, call records and so on but doesn't include drone data which is more complex and includes video, GPS coordinates, altitude and flight-path data, sometimes thermal or LiDAR readings, live-streaming with no fixed "original" recording, and cloud storage that might spread across different jurisdictions.[3]

These two laws were not drafted in relation to each other. *The Drone Rules,2021* were especially drafted to regulate airspace safety and doesn't deal with evidentiary integrity. The BSA was drafted to govern electronic records in a generic sense without specific contemplation about drone generated data which involves onboard flight controller, a removable storage card, a ground-control mobile application, and a cloud-hosted Digital Sky server, each under a different custodian and a different retention practice.

[1] Drone Rules, 2021, Schedule I (drone-category classification into Nano, Micro, Small, Medium and Large); IKIGAI Law, ibid.
[2] https://ksandk.com/litigation/section-63-bharatiya-sakshya-adhiniyam-2023/.
[3]https://www.researchgate.net/publication/395655381_The_Bharatiya_Sakshya_Abhiniyam_2023_Navigating_The_Complexities_of_Digital_Evidence_in_India's_Legal_Landscape

## II. Statement of the Research Problem

*The Drone Rules, 2021 and the Bharatiya Sakshya Adhiniyam, 2023* doesn't work together and doesn't expressly address the evidentiary treatment of drone generated data. Drone footage involves multiple layers such as the drone itself, its flight controller, a ground control app and a cloud server. *Section 63 of BSA, 2023* involves only a single identifiable device[4]. So, India has a separate rule for flying drones and separate provision for admitting electronic evidence, but nothing tells a drone operator or investigator how to preserve, certify and chain of custody of drone footage. The research problem determines whether and how this regulatory evidentiary gap can be bridged so that drone generated data can be authenticated, certified and admitted as digital evidence under Indian law. The central question is therefore not whether drone footage can be evidence. In principle, it can. The more difficult question is how drone-generated material should be proved when the material consists of multiple layers: the original sensor output, a memory card, a remote-pilot application, a cloud copy, an exported video, screenshots, metadata and a forensic report.

## III. Research Objective

1.To examine the regulatory framework governing drone operations under *the Drone Rules,2021* and to determine whether they impose any obligation on drone operators in relation to data generation, retention and disclosure.

2.To analyse *Section 63 of BSA* and to assess whether its certification procedure for electronic evidence accommodates the technical nature of drone generated data.

3.To identify the differences between drone captured evidence which includes geospatial metadata, flight-log correlation, live-streamed footage, and multi-jurisdictional cloud storage from conventional digital evidence.

4.To evaluate existing drone forensic literature to assess the practical challenges of chain-of-custody, authentication, and expert certification for aerial digital evidence.

5.To propose a model protocol for collection, preservation, certification and presentation of

[4] Bhatt & Joshi Assocs., Electronic Evidence Under BSA 2023: Section 63 Certificate Requirements & Supreme Court Interpretation (Sep. 25, 2026)

drone-generated evidence.

## IV. Research Question

1.What types of digital evidence can be generated by a drone system?

2.Whether *the Drone rules,2021* impose any obligation on drone operators regarding recording, preservation, integrity or custody of footage and flight data and do this obligation align with the condition prescribed under *section 63(2) of BSA*?

3.Whether Section 63 of BSA adequately capture the technical realities of drone-captured data, given that it was designed around single-device digital records like CCTV footage, call logs, and emails?

4.Whether the dual certification requirement under *section 63(4) of the BSA* requiring certification from device custodian and technical expert be practically satisfied for data distributed across a drone's onboard storage, ground-control application, and the Digital Sky Platform?

5.What regulatory and procedural reforms are necessary to bridge the DGCA's technical framework with the evidentiary demands of the BSA?

## V. Scope and Limitation of the study

### Scope

The study is confined to the civil-aviation regulatory framework applicable to unmanned aircraft systems in India such as *the Drone Rules, 2021*, and to the evidentiary framework under the *Bharatiya Sakshya Adhiniyam, 2023*, with particular focus on *Section 63* and the accompanying Schedule. A brief comparative reference to foreign jurisdictions (such as the US or UK) are included to identify possible reform models.

### Limitations

The paper is doctrinal which relies on statutes, case laws and secondary literatures and doesn't include empirical data such as interviews with law enforcement officials, drone operators, or forensic experts, which could have offered practical insight into how drone evidence is handled

on the ground.

The study is based on recently enforced legislation. So, there is limited judicial precedent interpreting *Section 63* in the context of drone generated evidence. Very few Indian judgments deal with drone footages as evidence.

Drone regulation and digital evidence law are both evolving areas particularly amid ongoing DGCA amendments and BSA-related jurisprudence still developing. The paper's analysis reflects the law as it stands as of the date of writing and may be affected by subsequent legislative or judicial developments.

**Research Methodology**

The study adopts doctrinal legal research. It relies on analysis of existing statutes such as the *Drone Rules, 2021, the Bharatiya Sakshya Adhiniyam, 2023, and the superseded Section 65-B of the Indian Evidence Act, 1872* and academic literatures on drone or unmanned aerial vehicles rather than field surveys, interviews, or empirical data collection. These sources were reviewed to identify the practical evidentiary vulnerabilities of drone-generated data that the legal framework must address.

The paper adopts an analytical and comparative approach which analyses *the Drone Rules, 2021 and the Bharatiya Sakshya Adhiniyam, 2023*. The rules relating to data generation, retention, and disclosure were mapped against the conditions for admissibility enumerated in *Section 63(2)* and the certification requirements in *Section 63(4) of the BSA* to identify points of correspondence and divergence. A comparative references to foreign jurisdictions such as the UK or US is used to identify possible models for reforms.

Data has been collected through internet-based research, using official government publications, statute databases, case-law repositories, and peer-reviewed or practitioner legal commentary.

The principal limitation of this method is that the paper doesn't include empirical data and is limited to publicly available legal materials and secondary commentary as of the date of writing.

## Literature Review

The evidentiary value of drone generated data have been studied in digital forensics engineering than in Indian legal writing.

Salamh, Karabiyik, Rogers and Matson conducted a comparative forensic examination of UAVs to identify “live” and “static” evidence traceability challenges to expose how inconsistent data integrity practices can compromise the repeatability of a drone forensic examination. They suggest a “UAV Kill Chain” to categorise the vulnerabilities. Their work demonstrates the fragility of chain of custody that Indian evidentiary doctrine is unequipped to test[5].

One review finds only two methods exist in the world for investigating drone evidence and both the methods work for only one specific drone model and not for every drones. Both the methods were criticized for not treating chain of custody. So, reviewers suggested a 3-step method (prepare – collect – analyse) to work on any drones[6].

Another paper developed a "forensic readiness framework" and pointed that police have to physically catch or disable a drone before they start investigation and that capture moment is itself a place where evidence changes hands with no counterpart in the BSA's Schedule[7].

A critical review titled "Who Watches the New Watchmen?" draws an explicit analogy between UAV and mobile-phone forensics which states that the access-exploitation techniques which is used to retrieve data from locked devices if uncontrolled can corrupt evidence and this risk is presently addressed in aviation regulation and requires a legal answer[8].

One study details the recovery of a real drone (DJI Phantom III) and pulled out its flight logs, sensor telemetry and control-module data using specific tools such as DatCon and DroneXtract documenting step by step chain of custody protocol as there was no official standard method

[5] F.E. Salamh, U. Karabiyik, M.K. Rogers & E.T. Matson, "A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges", 5(2) Drones 42 (2021), doi:10.3390/drones5020042.
[6] Research Challenges and Opportunities in Drone Forensics Models", 10(13) Electronics 1519 (2021), MDPI, available at https://www.mdpi.com/2079-9292/10/13/1519 (last visited 26 September 2026).
[7] A. Al-Dhaqm et al, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field", PMC, available at https://pmc.ncbi.nlm.nih.gov/articles/PMC8901304/ (last visited 26 September 2026).
[8] Who Watches the New Watchmen? The Challenges for Drone Digital Forensics Investigations", arXiv:2105.10917, available at https://arxiv.org/pdf/2105.10917 (last visited 26 September 2026).

to follow[9].

This literature converges on 3 findings. Firstly, Drone data comes from multiple sources unlike normal digital evidence which usually comes from just one device. Secondly, there is no single agreed upon forensic standard to investigate upon drone evidence. Thirdly, whether the resulting record can be certified and admitted in court of law which has been barely examined. It is this legal gap the paper research upon.

**Drone-Generated Digital Evidence**

A Drone is an unmanned aircraft operated remotely or autonomously using GPS, sensors, and AI-driven software[10]. *Rule 2(1)(i) of Drone Rules 2021* defines drones as "an unmanned aircraft system". Drone-Generated Digital Evidence is said to be any electronic or digital record that has been created, stored, transmitted or processed by a drone which is created directly by a sensor or indirectly by the system processing the sensor output. It includes visual records, Flight data, Telemetry, Device records, Operator records, Regulatory records, System-generated records, Forensic records and so on.

Drone generated data is not a single record and includes several connected records

- the sensor's original image or video file;
- the memory card or internal storage containing the file;
- a flight log generated by the flight controller;
- a remote-pilot application containing telemetry;
- a cloud account containing synchronised material;
- a Digital Sky record concerning registration or permission;
- a forensic image created by investigators; and

[9] Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone", 15(1) Journal of Cybersecurity and Information Management 197 (2025).
[10] https://mechtex.com/blog/what-are-drones-types-working-and-applications

- an exported copy or courtroom presentation file

**The Drone Rules,2021: An Airspace Centric Framework**

*The Drone Rules,2021* notified by the Ministry of Civil Aviation under *the Aircraft Act, 1934* were drafted to regulate the airspace within which Unmanned Aircraft Vehicle (UAV) operate, and they don't regulate the evidentiary status of drone recordings. The rules mainly deals with three things: who may fly (registration, the Unique Identification Number and Remote Pilot Certification) [11]where they may fly (the green/yellow/red zone map enforced through the Digital Sky Platform and the NPNT protocol),[12] and how the airframe itself must be built and equipped (Schedule II airworthiness standards and the mandatory safety features under Rule 11, such as anti-collision lighting, geo-fencing and real-time tracking).

*The Drone Rules,2021* defines the Digital Sky platform under *rule 3(1)(g)* as "online platform hosted by the Directorate General of Civil Aviation for various activities related to the management of unmanned aircraft system activities in India". The Drone rules require the unmanned aircraft system to be registered on the Digital Sky platform, and a Unique Identification Number is assigned. The UIN is linked with manufacturer's serial number and the serial numbers of the flight-control module and remote-pilot station which connects the particular recording to a particular drone, a particular flight-control system, a particular remote-pilot station and a particular owner or operator.

None of these provisions state about the aftermath of videos, photographs or telemetric data after being recorded through drones. There's no rule requiring footage to be kept for any minimum time, no rule requiring a "digital fingerprint" to be created the moment something is recorded (to later prove it wasn't tampered with), no standard format for flight logs that a court could rely on, and no rule saying who's responsible for the footage as it moves from the drone's memory card to a phone app and then to cloud storage. Penalties stated in the rules are only for contravening the flying rules not for mishandling the footage.

These rules were based on old aviation safety law which speaks about preventing crashes and

[11] Drone Rules, 2021, read with the registration and Unique Identification Number (UIN) requirements administered through the Digital Sky Platform; see "Understanding DGCA Drone Rules and The Digital Sky Platform", Skyglimps Technologies, available at https://skyglimps.com/understanding-dgca-drone-rules-and-the-digital-sky-platform/ (last visited 26 September 2026).
[12]Supra note 7. (reiterated)

airspace violations and not about courtroom evidence. The major issue is when the drone operator follows every rule including registration, getting Unique Identification Number, and so on but still his footage is not accepted as valid evidence in the court of law. That's because following the flying rules perfectly says nothing about whether the footage was protected from tampering along the way.

**The BSA, 2023: A Single-Device Paradigm**

The BSA defines “documents” and “evidence” to include digital and electronic records such as emails, server logs, messages and so on. A drone photograph, video, flight log, telemetry record would qualify as a document in accordance to relevancy. Evidence to be admissible in court must be relevant. So drone evidence must also be relevant to the fact in issue and its integrity and authenticity must be established.

*Section 63(1) of the BSA* treats information in an electronic record - whether printed, stored, recorded, or copied on optical or magnetic media, semiconductor memory, or other electronic means - as a document. This document is considered acceptable without needing the original, as long as certain conditions in the section are met. *Section 63(4)* says that when presenting a record, there must be a certificate that goes with it. This certificate should describe the record, how it was produced, the device used, and how it meets the conditions in *Section 63(2*).The certificate needs to be signed by the person responsible for the computer or communication device (or the relevant activity) and by a technical expert as specified in the attached schedule. The certificate is also expected to include a hash value to show that the record hasn't been changed.

The idea is that a single device or a small, identifiable group of devices under one person's control created the record, and one person can properly certify how that device works, while one expert can check the output. Drone data challenges this idea at almost every step. A single flight can create a video file on an SD card inside the drone, a separate telemetry log on the flight controller, a mirrored or live-streamed feed on a ground-control tablet app, and another copy or metadata record on the DGCA's Digital Sky server.That's four different "devices," each with a different person who could be seen as "in charge" (the drone owner, the remote pilot, the app host, and the Digital Sky administrator).None of them may have the technical ability to sign *a Section 63(4)(b)* certificate that explains how the electronic record was made. Live-streamed footage makes it even harder because if the stream isn't saved to a permanent storage,

there might not be an original copy to compare with later copies for verification. Cloud storage adds another layer of complexity because the data might be stored outside the state - or even outside India - where the legal case is being heard.

**Judicial Treatment of Electronic and Drone Evidence in India**

In *Anvar P.V. v P.K. Basheer*, a three-judge bench held that a certificate under *Section 65B(4) of the (then) Indian Evidence Act, 1872* was mandatory for the admission of secondary electronic evidence, and that no oral evidence could substitute for a missing certificate[13].A subsequent two-judge bench in *Shafhi Mohammad v State of Himachal Pradesh* introduced a competing view - that the certificate requirement could be relaxed in the interest of justice where the party relying on the record was not in a position to produce a certificate from a device it did not control.[14] The Supreme Court has separately emphasised that "source and authenticity are the two key factors" for electronic evidence generally.[15]

None of this jurisprudence has yet been tested against drone-generated evidence specifically.

**The Regulatory-Evidentiary Gap: Findings**

In *relating the Drone Rules,2021 with section 63(2) and 63(4) of the BSA*, certain principal findings are obtained.

**Statutory Silence on Aerial-Specific Evidentiary Protocols**

*The Drone Rules,2021* doesn't contain any rules to protect the reliability of the drone collected data. The provisions are only to protect people and not to prove the data is genuine. *Rule 17* prevents operators from sharing data with 3rd parties without the consent of the person the data concerns. "No Permission, No Takeoff" (NPNT) system and the Digital Sky Platform doesn't create a secure, verifiable record of the footage. The rules don't mention about hash value or any minimum period for keeping the data that is linked to litigation or limitation periods.

**The Certification Bottleneck under Section 63(4) of the BSA**

The provision states evidence would be admissible if it gets one certificate from a device

[13] Anvar P.V. v P.K. Basheer, (2014) 10 SCC 473, paras 20 and 24
[14] Shafhi Mohammad v State of Himachal Pradesh, (2018) 2 SCC 801
[15] Sanjaysinh Ramrao Chavan v Dattatray Gulabrao Phalke, (2015) 3 SCC 123, para 16

custodian and one from a technical expert. Since drone data is generated and stored across multiple devices there may be no single person competent to sign the certificate of evidentiary chain. This system creates problems for drone data. First, it is unclear which device should be certified. Second, drone operations are outsourced to third party or service provider, so it is unclear who is in charge of the data. Third, the hash value created says nothing about what happened to the data between capture and certification.

**Data Ownership, Consent, and the Privacy-Evidence Tension**

*Rule 17* protects the privacy of the people captured in drone footage. Neither the *Drone Rules nor the Bharatiya Sakshya Adhiniyam, 2023* explains how a court's power to call for electronic records fits with this consent requirement. It is therefore unclear whether an operator can refuse to hand over footage because the people in it have not consented, or whether a court order overrides *Rule 17*.[16]

**NPNT and Digital Sky as a Partial, Not Complete, Chain-of-Custody Safeguard**

The Digital Sky Platform is a system that keeps record of flight permission. It shows that a specific drone can fly at a stated time and place. This system doesn't prove the genuinity of the data. So the Platform can show that a flight was authorised, but it cannot show that the footage presented in court is the same as what the drone actually captured.

**Comparative Perspectives: United States and United Kingdom**

In the United States and United Kingdom, there is no specific law that states about admissibility of drone generated evidence, but they give a different perspective.

In US, constitutionality of drone evidence has been discussed. In *Long Lake Township v Maxon*, a local government repeatedly flew a drone over private property without a warrant. The Michigan Supreme Court held that even if this was an unlawful search, the drone footage could still be used as evidence, because the rule that excludes illegally obtained evidence does not apply in civil zoning-enforcement cases.[17]

In the United Kingdom, *the Air Traffic Management and Unmanned Aircraft Act 2021* gave

[16] Drone Rules, 2021, G.S.R. 589(E) (India), Rule 17
[17] Long Lake Township v Maxon, No. 164948 (Mich, 3 May 2024)

police officers a new power to ask a drone operator to show their registration, competence and identity documents at any time, even without suspicion.[18]

This comparative approach confirms that this is a first mover opportunity for Indian law to draft measures in relation to admissibility of drone evidence.

**Suggestions**

Amend *Schedule II of the Drone Rules, 2021* to introduce the Drone Evidence Certification Protocol. The Protocol shall include 3 components. First, every NPNT compliant drones shall compute a cryptographic hash of each recorded file at the moment of writing to onboard storage, and to transmit that hash - not the file itself, to avoid an unworkable bandwidth burden - to the Digital Sky Platform's servers as part of the existing post-flight reporting obligation already administered through that Platform. Second, whenever drone sends hash value the Digital Sky Platform would record it with timestamp to prevent tampering. Third, the schedule to BSA shall be amended to include drone specific certificate where the registered pilot would be the custodian of the data.

**Draft provision: admissibility of drone-generated electronic records**

The following is proposed as new *section 63A of BSA,2023* It addresses the admissibility of drone generated records with certification requirement.

SECTION 63A — ADMISSIBILITY OF DRONE-GENERATED ELECTRONIC RECORDS

(1) Notwithstanding anything contained in Section 63, where information contained in an electronic record is produced, in whole or in part, by an unmanned aircraft system as defined under the Drone Rules, 2021, such information (hereinafter "drone-generated data") shall be admissible in any proceeding as evidence of any contents of the original or of any fact stated therein, without further proof or production of the original recording device, if the conditions in sub-sections (2) and (3) are satisfied, in addition to the conditions specified in Section 63.

(2) The certificate required under Section 63(4) in respect of drone-generated data shall additionally state— (a) the unique identification number of the unmanned aircraft system, as

[18] Air Traffic Management and Unmanned Aircraft Act 2021 (UK), Sch 9

allotted under the Drone Rules, 2021; (b) the cryptographic hash value of the raw electronic record, generated at the earliest practicable point after capture, and, where the record has been transferred, copied, or transmitted thereafter, a hash value generated at each such stage; (c) the geospatial and temporal metadata, including the flight log, geo-fence coordinates, and telemetry data of the unmanned aircraft system for the duration of the recording, and a statement of the manner in which such metadata corresponds to the electronic record produced; (d) where the electronic record was stored, at any stage, on a server or system located outside India, the location of such server or system and the identity of the entity in control of it; and (e) a chronological record of every person or entity who has had custody or control of the electronic record between the time of its capture and the time of its production, and the manner in which such custody was transferred.

(3) Where the drone-generated data sought to be admitted was live-streamed, the certificate under sub-section (2) shall identify the point in time at which the live stream was first fixed in a stored, retrievable form, and any material discrepancy between the live-streamed transmission and the stored record shall be disclosed and shall be a relevant fact going to the weight, and not merely the admissibility, of the evidence.

(4) Where the certificate under this section is furnished in part by a person notified as an Examiner of Electronic Evidence under section 79A of the Information Technology Act, 2000 for the category "Drone Forensics," and no such Examiner is reasonably available to a party, the party may apply to the Court for an order directing examination by any other qualified expert, and the unavailability of a notified Examiner shall not, by itself, be a ground for excluding drone-generated data that otherwise satisfies this section.

(5) Where the hash values generated under sub-section (2)(b) at successive stages of custody are shown to be identical, there shall be a rebuttable presumption that the drone-generated data has not been altered between those stages.

(6) Nothing in this section shall be construed to affect the operation of the Digital Personal Data Protection Act, 2023 in respect of drone-generated data that constitutes personal data.

## CONCLUSION

Drone-generated digital evidence is likely to become increasingly important in Indian criminal

justice, civil litigation, regulatory enforcement, environmental governance and public administration. The BSA, 2023 provides a technologically neutral foundation by recognising electronic and digital records and regulating their proof. The Drone Rules, 2021 provide a regulatory architecture capable of establishing the identity of the drone, operator and flight.

The difficulty is that neither regime, operating alone, sufficiently addresses the complete evidentiary life cycle of a drone record. The Drone Rules focus on aviation safety and operational compliance; the BSA focuses on relevance, proof and admissibility. The evidentiary bridge must therefore be built through coordinated procedures concerning provenance, preservation, metadata, hash verification, expert testimony, certification and privacy.

A court should not treat drone footage as inherently reliable merely because it appears objective or machine generated. At the same time, it should not exclude technologically reliable evidence because the law has not yet developed drone-specific language. The appropriate approach is functional and evidence-based: identify the original record, establish the device and system that produced it, preserve its integrity, disclose the method of acquisition, satisfy section 63 where applicable and permit meaningful challenge.

The most important reform is the adoption of a standard drone-evidence protocol by the Ministry of Civil Aviation, the DGCA, investigative agencies and the judiciary. Such a protocol would convert regulatory data into usable evidentiary material while protecting privacy and fair-trial rights. The objective should not be to create a special law that makes every drone record admissible, but to create a reliable method by which courts can distinguish authentic, relevant and trustworthy drone evidence from altered, incomplete or misleading digital material.