
THE DIGITAL WILDLIFE BAZAAR: PLATFORM ACCOUNTABILITY FOR ILLEGAL ANIMAL TRADE IN INDIA

Pallavi Lakhera, Research Scholar, Faculty of Law, University of Allahabad, India

ABSTRACT

Illegal wildlife trade in India increasingly begins with a reel, listing or private message rather than a physical market. Public posts advertise protected birds, reptiles, live exotic animals and wildlife products; negotiations then move to direct messages, encrypted applications and online payments. Indian wildlife law can punish the seller, while information-technology law conditionally protects intermediaries that merely host third-party content. Neither framework clearly allocates responsibility when a platform recommends a suspicious listing, receives a precise report, preserves no usable evidence or repeatedly reconnects the same seller with buyers. This article argues against making platforms generally liable for every unlawful post or requiring indiscriminate monitoring of private communications. It instead proposes a graduated model based on platform function and knowledge. Public marketplaces and recommendation systems should bear stronger duties than encrypted messaging services. Once a sufficiently specific notice is received, an intermediary should preserve the listing and associated records, restrict the transaction, act against repeat offenders and cooperate with authorised investigators. The Wildlife Crime Control Bureau should operate a verified notice channel and publish species-linked red flags. Evidence preservation must accompany removal, because deletion alone may protect the trafficker and imperil the animal. This model aligns intermediary safe harbour with wildlife protection, privacy and reliable digital prosecution.

Keywords: online wildlife trade; intermediary liability; social media; digital evidence; Wildlife Protection Act; CITES.

I. INTRODUCTION

India's illegal wildlife market no longer depends on a visible shop. A seller can display an Indian star tortoise in an Instagram reel, describe monitor-lizard organs as a spiritual product, shift the conversation to a private message and arrange delivery without buyer and seller ever sharing a physical marketplace. In 2025, an alleged inter-State star-tortoise network was detected through an Instagram account that accepted online orders.¹ In another investigation, protected monitor-lizard body parts were advertised as *Hatha Jodi* through social-media and e-commerce pages; traders gradually removed public telephone numbers and redirected buyers to direct messages and WhatsApp.² The Directorate of Revenue Intelligence has likewise identified encrypted applications, closed groups, code words and temporary identities as features of contemporary wildlife trafficking.³

The legal difficulty is not simply whether the seller commits an offence. The Wild Life (Protection) Act, 1972 (WPA) already prohibits several forms of possession and trade and supplies powers of search, seizure and arrest.⁴ The harder question is what an intermediary must do when its infrastructure makes the transaction searchable, recommendable, payable or repeatable. Section 79 of the Information Technology Act, 2000 (IT Act) protects intermediaries that satisfy statutory conditions.⁵ That protection is essential: a platform cannot manually adjudicate the legality of every image, and a private messenger cannot inspect encrypted conversations without serious consequences for privacy and security. Yet safe harbour should not become operational indifference after a platform receives a precise report, profits from a promoted listing or permits a previously identified seller to return under a trivial variation of the same account.

This article advances a narrow claim. India should not impose general monitoring of all animal-related content. It should create a graduated duty that turns on the service performed, the platform's role in amplifying or completing the transaction and the quality of notice received.

¹ See *Four Held for Illegal Trade of Indian Star Tortoises on Instagram*, Times of India (Nov. 14, 2025), <https://timesofindia.indiatimes.com/city/ahmedabad/four-held-for-illegal-trade-of-indian-star-tortoises-on-instagram/articleshow/125308692.cms>.

² Wildlife Trust of India, *Continuing Online Trade of Monitor Lizard Body Parts: An OSINT and Maltego Case Study from India* (Mar. 2, 2026), <https://www.wti.org.in/feature/continuing-online-trade-of-monitor-lizard-body-parts-an-osint-and-maltego-case-study-from-india/>.

³ Directorate of Revenue Intelligence, *Smuggling in India Report 2024–25* 72 (2025), <https://dri.nic.in/writereaddata/smug2025/>.

⁴ Wild Life (Protection) Act, No. 53 of 1972, §§ 49B, 50–52, India Code (2025).

⁵ Information Technology Act, No. 21 of 2000, § 79, India Code (2000).

The proper sequence is **detect or receive notice, preserve, restrict, report and cooperate**. Removal without preservation can destroy evidence; preservation without welfare-oriented intervention can leave a live animal in danger. A workable regime must protect both the prosecution and the animal.

The analysis is doctrinal and problem-oriented. It reads the WPA together with section 79 of the IT Act, the Intermediary Rules, the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023. It also draws on Indian enforcement reports, recent field research and CITES guidance. The purpose is not to draft a new wildlife offence. It is to identify the point at which an intermediary's ordinary due-diligence obligations should become specific, time-bound duties in a wildlife case.

II. FROM PUBLIC DISPLAY TO PRIVATE DEAL

Online wildlife trade is not a single act performed on a single platform. It is a chain. Discovery may occur on a public feed, YouTube video, marketplace listing or search result. Negotiation moves to direct messages or encrypted applications. Payment and delivery may be arranged through separate services. Sellers use misspellings, local names, emojis and religious or medicinal descriptions to obscure the protected specimen. A platform may be passive at one point and active at another: it may merely store a post, recommend it to users interested in exotic pets, sell an advertisement, process payment or arrange logistics.

That functional distinction matters more than the label "social media platform." The same company may operate a public feed, a business catalogue, a paid advertising system and an encrypted messenger. A user who posts a photograph is supplying content. A platform that ranks the photograph for likely buyers, accepts payment to widen its reach or adds a purchasing interface does something more: it shapes the market in which the content becomes commercially effective. Liability should not arise merely because recommendation technology exists, but the platform's involvement is relevant when deciding what precautions are reasonable and whether its role remains confined to neutral transmission.

Online trade also reduces the value of conventional jurisdictional boundaries. The seller, buyer, payment account, server and animal may be in different States. A forest officer who identifies a listing may lack authority over the seller's location, while the platform may receive overlapping requests from police, WCCB, customs and State wildlife authorities. The National

Cyber Crime Reporting Portal already accepts suspicious social-media URLs, WhatsApp numbers and Telegram handles for cybercrime analysis.⁶ Wildlife enforcement should connect to this reporting architecture rather than build an isolated complaint system that investigators and platforms must learn afresh.

India's own enforcement practice recognises this migration. The Wildlife Crime Control Bureau (WCCB) has conducted successive Operation WILDNET exercises to identify online wildlife crime.⁷ A recent Indian study based on interviews with enforcement experts found that the WPA does not expressly address social-media-facilitated offences and that investigators face recurring problems of attribution, chain of custody and authentication.⁸ CITES also treats wildlife crime linked to the internet as crime enabled or facilitated through online services and asks parties to develop enforcement capacity and engage relevant platforms.⁹

The welfare consequences are easily lost in a debate framed only as cybercrime. Many listings concern living birds, reptiles and mammals. Delay can mean continued confinement, unsuitable temperature, dehydration, injury or death during transport. A platform's response must therefore do more than remove visible content. The response should preserve the digital trail and enable prompt identification and rescue. Conversely, automated deletion without human review can drive a seller into a closed group and erase the lead required to locate the animal.

III. THE PRESENT LEGAL FRAMEWORK

A. Wildlife law reaches the transaction but not platform design

The WPA regulates hunting, possession and trade in protected wildlife and wildlife articles.¹⁰ Sections 49B and 49C restrict dealings in specified animal articles and trophies, while sections

⁶ Indian Cyber Crime Coordination Centre, *Report Suspect to I4C*, National Cyber Crime Reporting Portal, https://cybercrime.gov.in/Webform/cyber_suspect.aspx (last visited Sept. 28, 2026).

⁷ Wildlife Crime Control Bureau, *Operation WILDNET-IV Report 1–4* (2021), <https://cites.org/sites/default/files/Wildnet%20IV.pdf>; Press Information Bureau, *Wildlife Crime Control Bureau Conducts Wildnet Operations in Noida, Seizes Wildlife Articles* (June 30, 2017), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1493592>.

⁸ Pradipty Bhardwaj, Jayadevan S. Nair & H.V. Girisha, *Legislative and Evidentiary Challenges Faced by the Indian Law Enforcement Agencies in Social Media-Enabled Wildlife Offences*, 18 J. Threatened Taxa 28874, 28875–76 (2026), <https://doi.org/10.11609/jott.10111.18.5.28874-28885>.

⁹ Convention on International Trade in Endangered Species of Wild Fauna and Flora, Resolution Conf. 11.3 (Rev. CoP19), *Compliance and Enforcement* 5–6 (2022), <https://cites.org/sites/default/files/documents/COP/19/resolution/E-Res-11-03-R19.pdf>.

¹⁰ Wild Life (Protection) Act §§ 9, 39, 44, 49B.

50 and 51 provide enforcement powers and penalties.¹¹ Attempts and abetment are separately punishable.¹² The 2022 amendment also created a domestic framework for specimens listed in the CITES appendices. Section 49M requires reporting and registration of living specimens of species listed in Schedule IV, supplemented by the Living Animal Species (Reporting and Registration) Rules, 2024.¹³

These provisions can reach a seller, possessor, transporter or person who intentionally assists the offence. They do not, however, provide a clear rule for recommendation engines, marketplace verification, repeat-seller controls or preservation of account records. Nor should ordinary hosting automatically become abetment. Criminal abetment requires a legally sufficient connection and mental element; the mere existence of an unlawful user post cannot establish it.¹⁴ The regulatory gap lies between automatic criminal liability and complete neutrality.

The Prevention of Cruelty to Animals Act, 1960 adds a welfare dimension where an animal is confined, transported or treated in a manner causing unnecessary pain or suffering.¹⁵ Nevertheless, it does not provide a digital notice system. Enforcement remains fragmented among forest departments, police, customs authorities, WCCB and animal-welfare bodies. A platform receiving a complaint may not know which authority can verify the species or secure the animal.

B. Safe harbour is conditional, not absolute

Section 79 protects an intermediary from liability for third-party information when its role is limited to providing access to a communication system and it neither initiates the transmission, selects the receiver nor modifies the information. Protection depends on observance of due diligence and is unavailable where the intermediary conspires, abets, aids or induces the unlawful act, or fails to act after legally cognisable knowledge.¹⁶

In *Shreya Singhal v. Union of India*, the Supreme Court read “actual knowledge” in section

¹¹ Id. §§ 49B–49C, 50–51.

¹² Id. § 52.

¹³ Id. § 49M & sched. IV; Living Animal Species (Reporting and Registration) Rules, 2024, G.S.R. 145(E), Gazette of India, pt. II sec. 3(i) (Feb. 28, 2024).

¹⁴ See Wild Life (Protection) Act § 52; Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 45–47, India Code (2023).

¹⁵ Prevention of Cruelty to Animals Act, No. 59 of 1960, §§ 3, 11, India Code (1960).

¹⁶ Information Technology Act § 79(2)–(3).

79(3)(b) as knowledge through a court order or notification by the appropriate government or its agency, rather than every private allegation sent to a platform.¹⁷ The ruling prevents private complainants from converting intermediaries into judges of lawful speech. The Delhi High Court similarly rejected an obligation of general ex ante monitoring in *MySpace Inc. v. Super Cassettes Industries Ltd.*, emphasising specific knowledge of identified material.¹⁸ At the same time, *Christian Louboutin SAS v. Nakul Bajaj* illustrates that an online marketplace's claim to neutrality weakens when it actively promotes, assures, packages or otherwise participates in a transaction.¹⁹

The IT Rules, 2021, as amended, require intermediaries to publish user rules, respond to lawful orders, preserve removed information and records for the prescribed period and maintain grievance and compliance mechanisms.²⁰ The Rules therefore provide useful procedural tools, but they are not adapted to wildlife listings. “Tiger claw,” “star tortoise” or a photograph of a caged parakeet may require species expertise. A notice that says only “animal content” is inadequate; a notice identifying the URL, account, suspected species, legal schedule and reason for suspicion can be acted upon and audited.

The same duty cannot apply identically to Instagram and WhatsApp. Public posts are searchable and may be algorithmically recommended. End-to-end encrypted private messages are not ordinarily visible to the service in intelligible form. Requiring routine scanning of private communications would collide with privacy and cybersecurity. *Justice K.S. Puttaswamy (Retd.) v. Union of India* requires state intrusions into privacy to satisfy legality, legitimate aim, necessity and proportionality.²¹ Platform accountability must therefore attach to information that the service actually processes or can lawfully preserve—not to a fictional ability to read every private message.

C. Removal and proof are different tasks

A wildlife prosecution may depend on a post that disappears within twenty-four hours, a deleted chat, payment metadata or an account registered with false particulars. The Bharatiya

¹⁷ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, 165–67 (India).

¹⁸ *MySpace Inc. v. Super Cassettes Industries Ltd.*, 2016 SCC OnLine Del 6382, ¶¶ 66–68, 80–81 (India).

¹⁹ *Christian Louboutin SAS v. Nakul Bajaj*, 2018 SCC OnLine Del 12215, ¶¶ 66–69, 76–78 (India).

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(b), 3(1)(d), 3(1)(g), 4(1), Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021), as amended through G.S.R. 120(E) (Feb. 10, 2026).

²¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, 509–10 (India) (plurality opinion).

Sakshya Adhiniyam, 2023 recognises electronic records and prescribes conditions and certification for their admissibility.²² A screenshot may show what a viewer saw, but it may not prove who controlled the account, when the content was created or whether the file was altered. Investigators need the original URL or account identifier, timestamps, associated subscriber information obtained through lawful process, preserved media, hash values and a recorded chain of custody.

The Bharatiya Nagarik Suraksha Sanhita, 2023 permits investigators and courts to require production of documents, electronic communications and communication devices where legally relevant.²³ These powers are valuable only if the platform retains the material long enough to respond. Content moderation and evidence preservation must therefore be designed together. Where a live animal faces immediate danger, the platform should preserve first and promptly restrict public access or transactional functions while notifying the competent authority. “Preserve first” does not mean leaving an unlawful sale online; preservation can occur through a secure internal copy unavailable to users.

IV. THE ENFORCEMENT GAP IS INSTITUTIONAL AS WELL AS LEGAL

The present system has several competent bodies but no single digital workflow. State forest departments investigate offences within their territories. WCCB coordinates intelligence and inter-State action. Customs and the Directorate of Revenue Intelligence intervene at borders and transport nodes. Police may possess better cyber-investigation capacity, while animal-welfare organisations may first identify an endangered live specimen. A platform cannot safely infer which of several emails represents an authoritative notice, and an officer cannot assume that a generic content-reporting form will preserve evidence for prosecution.

Operation WILDNET demonstrates that WCCB already has experience in online intelligence. The missing element is a standing interface with intermediaries: authenticated official accounts, standard notice fields, urgency labels, escalation contacts and auditable response times. CITES materials similarly emphasise national coordination, data collection, engagement with online platforms and cooperation across borders.²⁴ These are operational requirements,

²² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 & sched., India Code (2023).

²³ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 94, 105, India Code (2023).

²⁴ Convention on International Trade in Endangered Species of Wild Fauna and Flora, *Wildlife Crime Linked to the Internet*, https://cites.org/prog/imp/wildlife_crime_linked_to_the_internet (last visited Sept. 28, 2026); CITES Resolution Conf. 11.3, *supra* note 9, at 5–6.

not merely aspirations. A notice system that does not identify the species, listing, suspected offence and requested action will produce delay or excessive removal.

The gap is also temporal. A wildlife post may disappear after a few hours, yet a formal production order may take days. The Intermediary Rules require preservation of information and associated records after removal or loss of access, and lawful agencies may seek information through prescribed process.²⁵ Wildlife cases need a rapid preservation request that freezes existing records without immediately deciding criminal guilt. Such a request should be narrower than a disclosure order: it would prevent deletion while the authority obtains the necessary legal process. The distinction protects both investigation and privacy.

Finally, platforms and investigators measure success differently. A platform may count a deleted post as a completed moderation action. For enforcement, deletion may be the beginning of the case. Investigators need to connect the post to an account, device, payment trail, delivery location and ultimately the animal. Where an animal is alive, rescue speed is a separate measure. A credible framework should therefore track preservation, lawful disclosure, account disruption and welfare intervention rather than celebrate removal numbers alone.

V. WHY A GENERAL DUTY TO MONITOR WOULD FAIL

A universal proactive-monitoring obligation appears attractive but is legally and practically unsound. First, lawful and unlawful content often look alike. A conservation organisation, news report, zoo, registered holder and illegal dealer may post the same species. Automated systems can identify visual similarity but cannot reliably determine permits, provenance or intent. Over-removal would suppress education, rescue reporting and lawful conservation communication.

Second, private-message scanning would impose a disproportionate surveillance architecture. Wildlife enforcement does not justify weakening encryption for every user. The first-originator mechanism under the IT Rules is confined to specified serious purposes and operates through legal process; it is not a general licence to trace every suspected animal sale.²⁶

Third, excessive filtering can worsen enforcement. Sellers adapt by using code words, cropped photographs and closed groups. Evidence from India shows movement from public contact

²⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(g), 3(1)(h), 3(1)(j).

²⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).

details toward direct messages and multiple linked identifiers.²⁷ If platforms delete suspicious posts instantly and disclose nothing, investigators lose the path from advertisement to person, payment and location.

The alternative is not inaction. It is calibrated due diligence. A service that recommends a commercial listing, accepts advertising payment or repeatedly restores a known seller is differently situated from a messenger carrying encrypted content without access to its substance. Regulation should recognise that difference.

VI. A GRADUATED ACCOUNTABILITY MODEL

A. A verified wildlife notice

The WCCB should operate a standard electronic notice channel for cyber-enabled wildlife crime. State Chief Wild Life Wardens, designated forest officers and trained partner organisations could submit verified notices containing the URL, account identifier, suspected species or article, relevant legal provision, urgency and preservation request. Platforms should maintain a dedicated contact point and acknowledge such notices immediately. A private complainant could still report content, but coercive disclosure and final legal determinations would remain with authorised agencies or courts.

This approach respects *Shreya Singhal*: legal consequences would follow a notice from an appropriate government agency or a court, not an untested accusation. It would also reduce delay caused by notices sent to generic grievance channels.

B. Duties matched to platform function

Three levels are appropriate. **Hosting services** should enforce clear terms prohibiting illegal wildlife trade, provide reporting tools and act expeditiously on valid notices. **Public marketplaces and recommendation services** should additionally verify high-risk sellers, restrict paid promotion of protected species and use proportionate detection tools on public commercial content. **Transaction-enabling services** that process payments, provide “buy” functions or arrange delivery should retain seller and transaction records and suspend facilities

²⁷ Wildlife Trust of India, *supra* note 2; Bhardwaj, Nair & Girisha, *supra* note 8, at 28878–81.

attached to a verified illegal listing.

Encrypted messaging services should not be required to inspect message content. Upon lawful notice identifying an account or number, however, they should preserve available non-content records, prevent public business features from being used for a verified illegal trade and respond to valid production orders. This divides responsibility according to technical capacity and participation rather than brand name.

C. Preserve, restrict, report and rescue

A verified notice concerning a live animal should trigger four linked actions. First, the platform should preserve the identified content, account data and relevant logs in a secure form. Second, it should restrict the listing, payment link or promotional reach so that the transaction cannot continue. Third, it should report the action and available records to the requesting authority. Fourth, the authority should conduct a rapid welfare assessment and, where justified, rescue and place the animal under lawful care.

Preservation periods should be extendable through a reasoned legal request. Each transfer—from platform to investigator, investigator to forensic examiner and examiner to court—should record date, handler, hash value and storage medium. The section 63 certificate under the Bharatiya Sakshya Adhinyam should be prepared when the electronic record is produced, not reconstructed after authenticity is challenged.

D. Repeat offenders and transparent systems

Platforms should use reasonable account-linking indicators to prevent a seller removed after a verified wildlife offence from immediately returning. Relevant indicators may include previously used business contact details, payment identifiers and device or account signals, subject to data-protection safeguards and human review. Automated similarity should trigger review, not final guilt.

Large platforms should publish aggregate transparency data: wildlife-trade reports received, content restricted, records preserved, accounts disabled, response time and referrals to Indian authorities. No personal or investigative information need be disclosed. Aggregated reporting would reveal whether policies work without prejudicing prosecutions.

Finally, the WCCB should maintain a regularly updated list of code words, commonly misdescribed products and priority species for trained platform teams. CITES Resolution Conf. 11.3 encourages parties to develop internet-wildlife-crime capacity, share information and work with online platforms.²⁸ India's WILDNET experience provides an institutional foundation; what is missing is a stable, legally defined interface between that expertise and intermediary compliance.

VII. IMPLEMENTATION, SAFEGUARDS AND ACCOUNTABILITY

A. A notice must be precise and reviewable

A wildlife notice should not be a bare demand to remove "illegal animal content." It should identify the exact URL or account, the suspected species or wildlife article, the available reason for identification, the provision apparently engaged and the action requested. It should also distinguish among preservation, restriction, subscriber disclosure and emergency welfare assistance. The issuing officer's identity and authority should be digitally verifiable. A platform should record receipt, action taken and reasons for refusal or partial compliance.

Mistakes are inevitable because species identification from an image can be difficult and lawful possession may depend on registration, provenance or permits. Except where delay creates an immediate risk to a live animal or evidence, an affected user should receive notice and an opportunity to challenge the restriction. Review should be conducted by a person trained in wildlife classifications, not solely by a general moderation queue. Restoration should remain possible where the content concerns conservation education, journalism, rescue or a lawful registered specimen.

B. Data minimisation and controlled access

Evidence preservation can expose names, numbers, locations and communications of persons who have not committed an offence. The Digital Personal Data Protection Act, 2023 establishes a framework for lawful processing and reasonable security safeguards, but its substantive duties are commencing in phases.²⁹ A wildlife protocol should therefore limit preservation to records

²⁸ CITES Resolution Conf. 11.3, *supra* note 9, at 5–6.

²⁹ Digital Personal Data Protection Act, No. 22 of 2023, §§ 4, 8, 17, India Code (2023); Digital Personal Data Protection Act (Commencement) Notification, G.S.R. 843(E), Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025); Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, pt. II sec. 3(i) (Nov. 14, 2025).

reasonably connected with the identified account, listing and period. Access should be logged; data should be encrypted; disclosure should occur only under valid legal authority; and retained material should be deleted when the preservation period and lawful purpose end.

The same principle limits account-linking. A platform may compare business numbers, payment identifiers or device signals to detect the return of a verified seller. It should not create a permanent, opaque blacklist based on an untested public complaint. A match should prompt human review, and a user should be able to contest mistaken linkage. The objective is to prevent deliberate evasion, not to make automated suspicion irreversible.

C. Phased duties rather than an unfunded mandate

Implementation should begin with a pilot involving WCCB, selected State wildlife authorities, the Indian Cyber Crime Coordination Centre and major platforms. The pilot should test a common notice form, secure preservation channel and live-animal urgency protocol. Its first task should be practical: identify who answers a notice at 10 p.m. when a reptile is advertised for next-day delivery, which authority can reach the location and what minimum data the platform can lawfully preserve.

After the pilot, the Central Government could issue wildlife-specific due-diligence guidance under the existing intermediary framework or amend the Rules after consultation. Obligations should be proportionate to size, function and risk. A small discussion forum should not be expected to maintain the same systems as a significant social-media intermediary or a marketplace that processes payments. However, every service should publish a prohibition on illegal wildlife trade, provide an accessible reporting route and comply with valid preservation and production requests.

D. Metrics that test real outcomes

Public reporting should separate user complaints from verified government notices and should state median response times. It should also distinguish content removal, evidence preservation, account action and referral. Where disclosure is legally permissible, WCCB should publish aggregate figures on investigations initiated, animals rescued and cases in which digital evidence was usable in court. These figures would reveal whether the system merely cleans public feeds or actually disrupts trafficking.

Independent periodic review is equally important. False positives, species-identification errors, disproportionate data retention and discriminatory targeting should be examined alongside enforcement gains. CITES encourages parties to monitor trends and exchange information about internet-enabled wildlife crime.³⁰ India can contribute meaningful data only if platforms and authorities use compatible categories. A reviewable, evidence-based system is more defensible than either blanket immunity or blanket surveillance.

E. Safe harbour should reward a functioning system

The proposed model does not make a platform strictly liable whenever a trafficker succeeds in posting. Section 79 should continue to protect an intermediary that maintains the required systems, responds to valid notices and does not materially participate in the unlawful transaction. This preserves the central protection recognised in *Shreya Singhal* and *MySpace*: intermediaries should not lose safe harbour merely because they failed to discover every unlawful item in advance.³¹

The position changes when the service has specific lawful notice and does nothing, or when its own commercial conduct goes beyond neutral hosting. Repeated paid promotion of an identified seller, continued processing of a verified illegal transaction, destruction of preserved material or deliberate circumvention of a valid order should carry consequences. Depending on the facts, those consequences may include loss of section 79 protection for the identified material, regulatory directions, evidentiary inferences permitted by law or ordinary liability under an independently established cause of action. The violation must still be proved; safe harbour is a defence framework, not a substitute wildlife offence.

This calibrated approach also gives platforms predictable incentives. They know what information a valid notice must contain, what records must be preserved, which actions are urgent and how long restrictions may last. Authorities, in turn, cannot shift the entire burden of investigation to private companies. They must identify the suspected offence, use lawful process for disclosure and take responsibility for rescue and prosecution. Accountability becomes reciprocal rather than rhetorical.

³⁰ CITES Resolution Conf. 11.3, *supra* note 9, at 5–6.

³¹ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, 165–67 (India); *MySpace Inc. v. Super Cassettes Industries Ltd.*, 2016 SCC OnLine Del 6382, ¶¶ 66–68, 80–81 (India).

VIII. CONCLUSION

The digital wildlife bazaar is not located entirely on Instagram, WhatsApp or any single website. It is a sequence of public display, private negotiation, payment and delivery. Indian wildlife law can punish possession and trade, while intermediary law protects neutral hosting subject to due diligence. The present gap arises when a platform is neither the trafficker nor truly passive.

India should not solve that gap through indiscriminate surveillance or automatic platform liability. It should adopt a graduated model. Public commercial surfaces and recommendation systems should carry stronger preventive obligations; encrypted services should preserve and disclose only information lawfully available to them. A precise notice from a competent authority should trigger preservation, restriction, cooperation and repeat-offender controls. Where a living animal is involved, digital action must be connected to immediate welfare intervention.

Safe harbour should remain available to intermediaries that build and follow this process. It should become difficult to claim where a service knowingly promotes, monetises or repeatedly facilitates a verified illegal wildlife transaction. The goal is not to make platforms forest officers. It is to ensure that the design and speed of digital services no longer give wildlife traffickers an evidentiary and commercial advantage over the law.