

BEYOND CONTENT MATCHING: THE PROVENANCE GAP BETWEEN PLATFORM DETECTION AND CRIMINAL ATTRIBUTION IN INDIA'S NCII REGIME

by

Qinlei Wang¹

ABSTRACT

India's 2025 Standard Operating Procedure for non-consensual intimate imagery directs significant social media intermediaries to detect recurring content through hashes and, where onboarded, to communicate collated hashes to the Indian Cyber Crime Coordination Centre. The February 2026 amendment reduces the complaint-based removal period to two hours, while Rule 3(1)(g) separately requires preservation of removed information and associated records for 180 days. These measures create a discrete evidentiary problem. A content match may justify renewed removal yet provides no standalone account of the particular upload, the responsible account or the system that produced an evidentiary output. Through doctrinal analysis of the IT Rules, the 2025 NCII SOP, the Bharatiya Sakshya Adhiniyam and the decisions in *X v Union of India* and *Arjun Panditrao Khotkar*, this article identifies a provenance gap between the reusable detection fingerprint and the individual dissemination incident. It proposes a two-record protocol linking a restricted prevention identifier to a separately preserved, event-specific record of each removal, with source-system information, integrity data and a lawful export pathway supporting Section 63 certification. The analysis distinguishes existing duties from proposed implementation specifications and confines its claims to what public legal materials establish. The resulting approach maintains rapid protection while preventing evidence of similarity from being mistaken for proof of personal attribution.

Keywords: non-consensual intimate imagery; hash matching; electronic evidence; intermediary due diligence; Bharatiya Sakshya Adhiniyam; digital provenance

¹ Social Sciences graduate and researcher, King's College London, London, United Kingdom.

I. INTRODUCTION

The circulation of non-consensual intimate imagery presents two legally distinct events that platforms increasingly encounter in the same operational workflow. An individual may report the initial posting to secure immediate withdrawal from public access, while a later match against the reported content may trigger a second intervention concerning another URL, account or service. Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 requires reasonable and practicable measures within two hours after receipt of a qualifying complaint to remove or disable access to intimate, sexual, impersonating or artificially morphed material. G.S.R. 120(E), which entered into force on 20 February 2026, replaced the former twenty-four-hour period. The shortening of this response window intensifies the need to specify what records accompany each removal event.²

The November 2025 NCII Standard Operating Procedure supplies the distinctive factual and institutional setting. Developed following the Madras High Court proceedings in *X v Union of India*, the SOP instructs significant social media intermediaries to apply crawler or similar technology to hashes collated from reported imagery and envisages communicating those hashes to I4C through the Sahyog Portal where an intermediary has been onboarded. This prevention mechanism treats a reported digital object as a reusable detection signal, permitting prompt action when substantially similar imagery reappears through further sources. Its design addresses the recurring exposure identified in the litigation, although the legal significance of a future match differs from the significance of the first reported posting.³

The preservation duty runs alongside that prevention mechanism. Rule 3(1)(g) requires an intermediary removing or disabling information on specified grounds to retain the information and associated records for 180 days for investigation, subject to longer retention required by a court or lawfully authorised government agency. Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023 regulate the proof of electronic records, and the scheduled certificate addresses digital-record source, system operation and integrity information. The Rules consequently require retention at the institutional point when access ends, while evidence law evaluates a later output generated from a particular system. The legally consequential unit of

² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b), as amended by Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India); Ministry of Electronics & Information Technology, Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, at 1 (2026).

³ *X v. Union of India*, W.P. No. 25017 of 2025, orders dated July 15 and Oct. 22, 2025 (Madras H.C.); Ministry of Electronics & Information Technology, Government of India, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content 6–8 (Nov. 2025).

proof may therefore be an identifiable uploading or moderation event rather than the fingerprint that first prompted detection.⁴

This article isolates a specific omission in the interface between those instruments. The 2025 SOP prescribes hash-based recurrence prevention, and Rule 3(1)(g) prescribes general preservation, yet the publicly specified NCII workflow leaves the status of a match-linked incident record unresolved. A fingerprint may support a moderation decision about similar content while remaining insufficient to establish a particular account's dissemination, a person's authorship or the provenance of an electronic record tendered in proceedings. Treating these propositions as equivalent risks both evidentiary overclaim and an avoidable dependence on victims to reconstruct the history of posts already removed from view.

The proposed response is a two-record protocol built around incident provenance. One record holds the detection reference used to identify reappearances, with its algorithm and matching status expressly distinguished from criminal proof. A second record documents each platform-specific content instance, its available account and post identifiers, timestamps, removal basis, integrity information and lawful export history. The relationship between those records permits investigation of a recurring image while leaving attribution and admissibility open to independent evidentiary scrutiny. It also permits privacy safeguards to govern intimate files differently from operational fingerprints, avoiding an unnecessarily extensive shared archive.

Research on image-based sexual abuse has established the importance of dignity, consent and access to remedy. McGlynn and Rackley's account of image-based sexual abuse broadens the harm beyond a narrow category of retaliatory disclosures, while Henry and Witt analyse the inadequacies of platform governance and the burden placed upon individuals reporting abuse. Hörnle's 2026 analysis connects criminal law with platform duties, and Huber documents procedural weaknesses in policing responses. Their work makes the institutional distribution of responsibility unavoidable; the present analysis extends that insight to the particular record produced when a platform identifies reappearing imagery through a hash. Indian evidence doctrine, including the Supreme Court's directions in *Arjun Panditrao Khotkar* concerning

⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(g) (India); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 & sched. to § 63(4)(c) (India).

metadata and segregated preservation, supplies an additional and directly relevant starting point.⁵⁶

The method is a source-bounded doctrinal reading of the 2021 IT Rules as amended in February 2026, the November 2025 NCII SOP, the Bharatiya Sakshya Adhiniyam and the identified judicial decisions, combined with a narrowly specified institutional design proposal. The analysis compares legal triggers, custodial responsibilities and inferential limits across the complaint, detection, preservation and production stages. Neither the existence of an I4C hash bank nor an obligation to preserve records establishes the internal fields actually held by any platform; conclusions about real-world noncompliance, algorithmic performance or the evidentiary quality of particular prosecutions would require additional empirical material. That limitation is essential to the claim advanced here, which concerns the content of a publicly prescribed process rather than an asserted pattern of undocumented operational failure.

II. TWO DISTINCT DUTIES IN THE NCII LEGAL FRAMEWORK

A. Complaint-Based Removal and Recurrence Prevention

Indian law regulates NCII through a dispersed architecture in which criminal law, intermediary regulation, evidence law and constitutional doctrine perform distinct functions. The Information Technology Act, 2000 remains important through provisions addressing privacy violations and the publication or transmission of obscene or sexually explicit material in electronic form.⁷ Section 66E addresses intentional or knowing capture, publication or transmission of images of a private area under circumstances violating privacy, while Sections 67 and 67A criminalise specified forms of obscene and sexually explicit electronic publication or transmission. The Bharatiya Nyaya Sanhita, 2023 adds offences including voyeurism under Section 77, which covers dissemination of an image of a woman engaging in a private act in specified circumstances.⁸ These provisions establish substantive liability while leaving continued online availability to be addressed through intermediary and remedial mechanisms.

⁵ See Clare McGlynn & Erika Rackley, Image-Based Sexual Abuse, 37 Oxford J. Legal Stud. 534, 534–61 (2017); Clare McGlynn, Erika Rackley & Ruth Houghton, Beyond “Revenge Porn”: The Continuum of Image-Based Sexual Abuse, 25 Feminist Legal Stud. 25, 25–46 (2017); Nicola Henry & Alice Witt, Governing Image-Based Sexual Abuse: Digital Platform Policies, Tools, and Practices, in The Emerald International Handbook of Technology-Facilitated Violence and Abuse 749, 749–68 (Jane Bailey, Asher Flynn & Nicola Henry eds., 2021).

⁶ See Julia Hörnle, Fighting the Beast of Image-Based Sexual Abuse. Part 1—the Criminal Law and Platform Regulation, 34 Int’l J.L. & Info. Tech. eaag006 (2026); Antoinette Raffaella Huber, Image-Based Sexual Abuse: Legislative and Policing Responses, 25 Criminology & Crim. Just. 736, 736–52 (2025).

⁷ Information Technology Act, No. 21 of 2000, §§ 66E, 67, 67A, 79 (India).

⁸ Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77 (India).

Intermediary due diligence supplies the principal rapid-removal mechanism. Rule 3(2)(b) is distinctive in allowing urgent action against qualifying intimate or impersonating content without requiring the victim first to obtain a final judicial determination. The provision recognises that delay can be constitutive of harm. Every additional hour of public availability can create new downloads, mirrors, reposts and search results, making later removal progressively less complete. The reduction from twenty-four hours to two hours in 2026 therefore represents a significant reordering of regulatory time. It treats certain privacy and sexual harms as requiring an accelerated response qualitatively different from ordinary content disputes.⁹

The Government's 2025 SOP develops the grievance process established during *X v Union of India* by describing routes through intermediaries, the National Cyber Crime Reporting Portal, law-enforcement agencies and One Stop Centres. For significant social media intermediaries, paragraph 3 of the intermediary instructions requires crawler or comparable technology to identify hashes associated with reported NCII, takedown of similar content across other URLs and sources, and communication of collated hashes to I4C through Sahyog where onboarded. It also requires periodic information to the affected person about the removal of reported and resurfaced content. These provisions are operationally significant, although their language identifies neither a required record schema for each subsequent match nor a procedure that would connect the hash-bank entry to an authenticated record of a particular later upload. The SOP reproduces the former twenty-four-hour period, whereas the amended Rule 3(2)(b) prescribes two hours; the SOP itself disclaims any power to modify the Rules and calls for verification of the latest version.¹⁰

The Madras High Court's final order in X v Union of India explains the protective rationale for recurrence prevention. After recording the SOP and the risk of further resurfacing, the Court contemplated prompt blocking of additional appearances without making the petitioner commence fresh litigation for every incident. Its direction to publicise the SOP and provide diligent assistance grounds the system in practical accessibility and dignity under Article 21. The order does not establish that a match from a prevention system proves who uploaded the material, nor does it prescribe the platform-side evidence package for a subsequent criminal

⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b), as amended by G.S.R. 120(E) (Feb. 10, 2026) (India), effective Feb. 20, 2026.

¹⁰ Ministry of Electronics & Information Technology, Government of India, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content 6–8 (Nov. 2025); Press Information Bureau, Ministry of Electronics & IT, MeitY Issues Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content (Nov. 11, 2025).

*proceeding. That remaining evidentiary function must be identified within the governing legislation and evidence law.*¹¹

B. Preservation and Legal Production

The same IT Rules that accelerate removal also contain a preservation obligation with different temporal logic. Rule 3(1)(g) provides that where information has been removed or access has been disabled on specified grounds, the intermediary shall preserve the information and associated records for 180 days for investigation purposes, or longer if lawfully required, without vitiating the evidence. This language is exceptionally important for NCII. It means that removal from the interface should not ordinarily entail deletion from every system under the intermediary's control. Public unavailability and evidentiary retention are legally separable states.

The phrase “associated records” is potentially broad and valuable, yet the Rules leave its NCII-specific content unspecified. Depending on the platform and facts, relevant records may include upload timestamps, account identifiers, content identifiers, complaint records, moderation actions, hashes, metadata, re-upload matches and records of links or accounts through which material travelled. The preservation rule leaves an NCII-specific minimum record set unenumerated. A platform could therefore comply with the general duty while preserving information in a form that is less useful for later proof, particularly where identifiers or contextual metadata become detached from the retained content.

Under Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, digital records receive statutory recognition while the admissibility of a computer output depends upon prescribed conditions. Section 63(2) addresses ordinary-course system use and operation; subsection (3) expressly contemplates interconnected systems and processing through an intermediary; subsection (4) requires a certificate when an electronic record is submitted under that provision. The Schedule separates the party's declaration from the expert's declaration and calls for digital-source particulars and hash reports. A cryptographic hash assists verification of the integrity of the specified output, whereas a matching fingerprint generated for moderation provides a different proposition concerning apparent content identity or similarity. Preserving one form of hash supplies no substitute for documenting the other or for authenticating a source-specific platform export.¹²

¹¹ X v. Union of India, W.P. No. 25017 of 2025, ¶¶ 9–10 (Madras H.C. Oct. 22, 2025).

¹² Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(2)–(4) & sched. to § 63(4)(c) (India), <https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf>.

The legal transition therefore concerns evidentiary meaning as well as retention. A complaint initially seeks withdrawal of the exposed content, while a subsequent investigation may need to establish the appearance of a given object at a particular account and time. Screenshots supplied by an affected person may assist that inquiry, although their available context differs from server-side posting records and moderation logs. Section 63 certification is an evidentiary process undertaken when an output is tendered, while Rule 3(1)(g) governs retention at an earlier stage. A workable preservation architecture should keep those functions separate and maintain sufficient source information to permit legally adequate production when requested.¹³

This requirement also has an established judicial precursor. In *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, the Supreme Court addressed practical difficulties with electronic evidence held by third-party systems and directed attention to secure segregation, metadata preservation, retrieval and production under Section 67C of the Information Technology Act. That judgment concerned the former Section 65B framework, so its directions inform the broader preservation problem while the 2023 *Bharatiya Sakshya Adhiniyam* supplies the applicable statutory text for the present analysis. The contribution developed here accordingly concerns the narrower category of a matched NCII reupload and the incident-specific proof absent from the prevention-oriented SOP, rather than a new general proposition that intermediaries should retain electronic records.¹⁴

III. THE PROVENANCE GAP CREATED BY MATCHED CONTENT

A. Content Identity and Incident Identity

The principal difficulty appears at the second dissemination event. A platform may identify a newly appearing file through a hash linked to an earlier NCII complaint and remove the matched content in order to prevent renewed injury. Yet the match expresses a relationship between digital objects, while a criminal allegation about distribution requires an account of conduct at a particular time and source. Treating the result of detection as an adequate substitute for the incident record would allow the same hash-bank reference to conceal legally material differences between separate uploads, account operators, transformations and moderation decisions. The distinction is heightened by the two-hour complaint-removal rule,

¹³ *Bharatiya Sakshya Adhiniyam*, No. 47 of 2023, § 63(1)–(4) (India).

¹⁴ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1, ¶¶ 62–63, 72(c)–(d) (India); *Information Technology Act*, No. 21 of 2000, § 67C (India).

which gives the platform an immediate safety objective while leaving investigators to establish the event later.

Reupload detection intersects with the February 2026 rules concerning synthetically generated information, although the obligations must be read with their distinct scopes intact. Rule 3(3)(a)(i) addresses unlawful synthetic material including non-consensual intimate imagery, whereas the labelling and permanent-metadata language of Rule 3(3)(a)(ii) applies to other synthetically generated information outside that prohibited category. The amendment accordingly supplies no general guarantee that unlawful synthetic NCII carries a provenance label at the point of removal. Where an intermediary lawfully possesses generation, modification or processing metadata, those records may assist in explaining an incident; the existence of such records should be established rather than assumed. This legal distinction reinforces the need for a record tied to the specific posting and its moderation history.¹⁵

A match identifies a candidate relationship between items of content; its inferential significance depends upon the matching technique, the threshold employed and any review subsequently undertaken. An exact cryptographic match may support byte-level identity between two specified files, while a perceptual or similarity match has a different, often probabilistic or threshold-dependent basis. Neither method independently determines whether an account operator created the image, knowingly distributed it, obtained consent or satisfied an offence's mental element. These propositions remain open even where an automated match justifies precautionary withdrawal of content. A legally meaningful incident record must preserve each platform event as an independently identifiable occurrence and preserve the technical reason why the content was associated with a previous report.¹⁶

B. The Three Evidentiary Objects

Electronic evidence in platform cases is often discussed as though the relevant object were a single file. NCII disputes demonstrate why that model is incomplete. The image or video may be important, yet its legal meaning depends on a network of records concerning where it was uploaded, by which account, when it was made available, how it was modified, which users or systems reproduced it, when the intermediary received notice and what action followed. The evidentiary object is therefore relational. A preserved file without platform context may prove

¹⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(3)(a)(i)–(ii), as inserted by G.S.R. 120(E) (Feb. 10, 2026) (India).

¹⁶ Ministry of Electronics & Information Technology, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content 7 (Nov. 2025).

the existence of intimate material while doing little to establish a particular act of dissemination or an intermediary's response to a complaint.

The Bharatiya Sakshya Adhiniyam accommodates this broader understanding by treating electronic and digital records as documents and by requiring attention to the source from which an electronic output is produced. The certificate contemplated by Section 63 supplies a statutory framework through which production, source and integrity can be described; judicial assessment of relevance, authenticity and the inferences drawn from the record remains separate. The inclusion of hash values in the Schedule is particularly significant for content capable of being copied, transformed or reproduced across systems.¹⁷ A hash can help demonstrate that a preserved object is identical to an earlier object, although perceptual matching systems used for modified images may operate through different techniques and should not be conflated with cryptographic hashing for integrity.

Platform custody raises a further issue since the intermediary may be the only actor capable of preserving contextual records. A victim can capture a screenshot and copy a URL, yet ordinarily lacks access to backend timestamps, internal content identifiers, moderation logs and records concerning account authentication. Law enforcement may later request such information, with availability determined by the records the platform retained and can reliably export. The 180-day rule therefore performs an access-to-justice function. It preserves the possibility that evidence outside the victim's control will remain available long enough for an investigation to engage with it.

This function becomes more important where different services participate in the same chain of dissemination. A synthetic intimate image might be generated on one service, uploaded to another, redistributed through messaging applications and indexed by search systems. No single intermediary can preserve the complete history. Evidentiary continuity should consequently be modular. Each service should retain the records within its lawful control in a form capable of later combination with records from other sources. The legal objective is not an impossible universal chain of custody beginning at creation. It is a reliable local chain for each institutional custodian.

The concept of source should also be handled carefully. In digital-evidence law, source can refer to the device or system from which an output was produced. In an NCII investigation, investigators may use "source" colloquially to mean the person who originated the content. These are different questions. A platform export can establish that a record came from a

¹⁷ Id. sched. to § 63(4)(c). Cryptographic hashing for integrity should be distinguished from perceptual or similarity hashing used to detect modified content.

specified platform system without proving that a particular human being created the intimate image. Good evidentiary design should preserve this distinction so that technical provenance is not overstated as authorship or culpability.

The legal materials therefore disclose three evidentiary objects that ought to be separately represented. The first is the reported or retained image, whose cryptographic digest and custodial history may help identify a stable digital object. The second is the operational fingerprint used to detect potential reappearances, where the matching method, algorithm version and basis of any similarity decision bear upon the meaning of a match. The third is an event record drawn from the intermediary that processed a particular upload, containing the information actually held about posting, account association, availability, notice, detection and moderation. These objects may be linked through a controlled identifier, yet each supports a different proposition and may have a different legitimate retention and disclosure basis. Their separation supplies the conceptual mechanism missing from a proposal concerned solely with storing the removed image.

C. What the Public SOP Specifies and Leaves Open

The absence identified here is documentary and confined. The published 2025 SOP directs SSIMs to detect resurfacing, distribute collated hashes under specified conditions and notify the complainant of removal, while Rule 3(1)(g) mandates retention of information and associated records following defined removal actions. The SOP supplies no public minimum incident schema identifying the matched upload, the platform system holding relevant records, the hash type used for detection or the evidentiary status of a positive match. This conclusion establishes an under-specified procedural interface, rather than proving that intermediaries fail to maintain such information internally. It also leaves room for safeguards proportionate to the different functions of a prevention register and an investigation-ready incident record.¹⁸

IV. THE INCIDENT PROVENANCE STANDARD

A. A Separate Preservation Trigger for Each Removed Instance

Rule 3(1)(g) already links specified forms of removal or access restriction to preservation of information and associated records, making a new freestanding statutory retention duty an

¹⁸ Ministry of Electronics & Information Technology, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content 7–8 (Nov. 2025), <https://www.meity.gov.in/static/uploads/2025/11/a2c9500ef5f8b62a43bfc68747de592d.pdf>; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(g), 3(2)(b) (India).

unnecessarily expansive starting point. For a qualifying Rule 3(2)(b) complaint, the platform should record a preservation event contemporaneously with disabling access. Where a later match leads to removal, the platform should assess the applicable Rule 3(1)(g) trigger for that separate action, including voluntary removal of material violating Rule 3(1)(b) where relevant. A matching signal in isolation should never be represented as an automatic legal finding against an uploader. Once the later item is actually removed on a covered ground, its separate event record should identify the new instance and reference the original prevention case, subject to the intermediary's lawful control of relevant data.¹⁹

B. Minimum Fields and Their Evidentiary Purpose

The phrase “associated records” provides the doctrinal opening for an incident-centred specification. For each removed instance, a minimum record could include the platform-received object if lawfully held, its cryptographic integrity digest, a unique post or content identifier, the relevant URL or service location, upload and moderation timestamps, complaint or detection pathway, account identifier where available, and an immutable sequence of material preservation and export actions. A match-linked instance should additionally identify the originating prevention reference, matching method, version and recorded outcome of any manual review. System-generated timestamps require a stated time standard and should be described as platform records rather than conclusive evidence of human action. This minimum is justified by the legal propositions an investigator may later seek to prove, with supplementary collection determined by relevance, data availability and lawful authority.²⁰

The schema also requires a record of uncertainty. A similarity system may operate with platform-defined thresholds that are unavailable in public documentation, and an account identifier may reflect a service login rather than verified personal identity. An incident export should therefore state which fields derive from ordinary platform activity, which were generated by automated detection, which result from human review and which are unavailable. This classification constrains inferential inflation at the point where a file is placed in investigative custody and gives parties a basis for challenging the accuracy or relevance of a match. The proposal does not oblige platforms to collect biometric, identity or behavioural information merely to satisfy an expansive theory of future evidentiary usefulness.

¹⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(b), 3(1)(g), 3(2)(b) (India).

²⁰ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4) & sched. to § 63(4)(c) (India).

C. Custodial Separation and a Legally Reviewable Export

Section 63 supplies a legal reason to distinguish operational matching from a source-specific export. When the intermediary receives a lawful production request, an appropriately authorised custodian should identify the source system, the retained object or records actually produced, the relevant processing history and the hash algorithm applied to that output. The Schedule's separate party and expert declarations should inform export readiness without being presented as certificates already completed by a moderation system. The same framework requires preserving the relationship between an earlier complaint reference and each new incident, while avoiding an assumption that a unified or distributed technical system proves the identity of the human uploader. Judicial scrutiny of authenticity, relevance and probative weight remains available after the record enters proceedings.²¹

This standard imposes a useful boundary on the proposal's institutional ambitions. The intermediary retains and describes records generated in the ordinary operation of its service and its compliance process, while law-enforcement bodies establish the broader sequence of offending conduct through legally authorised investigation. A hash-bank administrator may retain the shared prevention reference and information necessary to manage it, but the platform that handled a particular post remains the appropriate source for that event's contextual account records. In this allocation, the prevention system locates candidates, the intermediary documents specific events and the court determines the evidentiary implications of authenticated outputs.

V. PROPORTIONALITY AND PROCEDURAL RIGHTS

Preserving intimate content creates its own privacy risk. Evidence retention must therefore be governed through strict role-based access, audit logging and purpose limitation. Retention for investigation supplies no basis for routine employee access or a broadly accessible internal archive. The Madras High Court's concern with investigative re-exposure illustrates why access design is part of substantive protection. Systems should minimise the number of people who must view the content, favour hash and metadata operations where visual inspection is unnecessary, and provide specialised procedures when viewing is unavoidable.

Victims should receive meaningful confirmation that a qualifying takedown has occurred and that relevant evidence has been preserved for the applicable period, subject to lawful disclosure rules. Such a receipt would reduce uncertainty and the felt necessity to maintain private copies indefinitely. It could identify the complaint reference, date, platform action,

²¹ Id. § 63(2)–(4), sched. to § 63(4)(c).

preservation period and route for law-enforcement follow-up without reproducing the intimate image. This small procedural reform would translate backend retention into survivor-facing legal security.

An incident-centred preservation protocol must begin from legal purpose and necessity. Rule 3(1)(g) establishes a 180-day investigative preservation requirement and expressly permits longer retention where the specified authorities lawfully require it; it is therefore a baseline period with an extension mechanism, rather than an absolute maximum applicable to every copy or record. The protocol should separately record the statutory preservation period, the grounds of any legal hold and the legal basis governing continued retention after those obligations lapse. This distinction prevents a general concern for future litigation from being treated as an indefinite authorisation to archive intimate images.²²

The second requirement is proportionality. Preserving an intimate file may be necessary, while duplicating it across internal teams or permitting broad access would exceed that evidentiary purpose. Technical design should separate integrity operations, which can often be performed through hashes or automated processes, from occasions requiring human viewing. Audit trails should record access to retained material, and the system should support investigation through metadata where substantive content is unnecessary for a particular step. Proportionality therefore concerns the internal life of evidence as well as the decision to preserve it.

Purpose limitation becomes especially important once matched-content detection relies upon shared infrastructure. The presence of a hash in a prevention bank supplies no general permission to share the underlying intimate image with a wider institutional audience, nor does retention for investigation authorise secondary processing for recommendations, advertising or model development. Where identifying or complaint data are linked to a hash, access should be restricted to personnel and agencies with a defined role and a lawful basis. A prevention identifier may persist under a justified safety function even when an underlying image follows a different retention pathway; the conditions for each should remain transparent and independently reviewable.

The fourth requirement is procedural intelligibility. A victim should be able to understand what has happened after a complaint without learning the internal architecture of the intermediary. The platform can state that content has been disabled, that relevant records are retained for the statutory period, that they will be disclosed only through lawful channels, and

²² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(g) (India).

that the victim may provide the complaint reference to law enforcement. Intelligibility reduces uncertainty and can prevent repeated reporting motivated by fear that removal destroyed the evidence.

The Madras High Court's approach in *X v Union of India* situates rapid action within the dignity protected by Article 21, especially where renewed circulation would otherwise force repeated petitions for relief. That concern extends to the institutional handling of material preserved after takedown. A process that requires complainants to repeatedly retrieve, view or redistribute intimate evidence may reproduce procedural harm even when investigators are pursuing a legitimate case. Event-specific backend preservation allows the platform's technical custody to support later lawful requests while limiting the evidentiary burden imposed on the person who originally sought removal.²³²⁴²⁵

Procedural justice also requires attention to informational control. Once a victim reports NCII, material may enter several institutional systems including platform moderation, law enforcement, prosecution and courts. The victim's capacity to control those transfers is necessarily limited; the state and intermediaries can still reduce unnecessary circulation through purpose limitation and secure custody. The legal distinction between preservation and access is fundamental. A duty to retain evidence creates no corresponding entitlement for unlimited actors to view it. This distinction should be explicit in SOPs, platform practices and investigator training.

Synthetic media also reinforces the need to separate authenticity from consent. An authentic intimate photograph can be distributed without consent, while a synthetic image can violate dignity despite never having been an authentic record of the victim's conduct. Evidence systems should therefore avoid treating proof of manipulation as proof that no legally cognisable sexual harm occurred. Relevant questions include who created or disseminated the material, what privacy or sexual interests were invaded, and how the platform responded after notification. The 2026 regulatory emphasis on synthetic media should strengthen the consent-centred logic of NCII protection while adding provenance-sensitive duties.

VI. IMPLEMENTATION THROUGH THE NCII SOP

The existing NCII SOP provides a plausible institutional location for a supplementary incident-provenance annex, although the extent of any binding obligation would depend upon

²³ *X v. Union of India*, W.P. No. 25017 of 2025, ¶ 10 (Madras H.C. Oct. 22, 2025).

²⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

²⁵ *X v. Union of India*, W.P. No. 25017 of 2025, ¶¶ 9–10 (Madras H.C. Oct. 22, 2025); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

the legal instrument eventually adopted. Such an annex should distinguish duties established by the IT Rules from technical recommendations intended to make compliance auditable. It should also correct the SOP's superseded twenty-four-hour statement and retain the conditional qualification attached to use of the Sahyog Portal. Administrative guidance could standardise event identifiers, field definitions and custodial handoffs, while a binding expansion of intermediary obligations would require an appropriate legal basis and procedural scrutiny.²⁶²⁷

Coordination acquires particular importance as a victim's experience crosses institutional boundaries. A platform may remove a post, the NCRP may receive a complaint, state police may investigate, and a court may later assess electronic evidence. Each institution can perform its own function correctly while the overall pathway still fails if identifiers, timestamps or records cannot be matched across systems. A shared complaint or preservation reference would reduce this fragmentation. It need not create a single national database of intimate images. The reference can connect separately held records while allowing each custodian to maintain its own security and access controls.

Training should accompany technical standardisation. Investigators require guidance on requesting platform records before retention periods expire, preserving received data, obtaining appropriate certificates and avoiding unnecessary victim exposure. Platform grievance teams require guidance on when a complaint falls within Rule 3(2)(b) and how the preservation trigger interacts with ordinary moderation workflows. Prosecutors require sufficient technical understanding to explain the relationship among screenshots, platform exports, hashes and source-system records. The value of a standard format is realised only where institutional actors understand what its fields mean.

The existing division between reupload prevention and evidence preservation supports a two-record workflow. A prevention register can contain hashes and associated abuse-report references for locating further appearances, while the platform handling each matched post preserves its own event-specific information and logs the link between the match and the resulting action. Algorithm descriptions and any applicable match threshold should accompany the local incident record where available, enabling subsequent review of the

²⁶ Ministry of Electronics & Information Technology, Government of India, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content (Nov. 2025).

²⁷ Ministry of Electronics & Information Technology, Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content 4, 7 (Nov. 2025).

classification that initiated withdrawal. This design preserves the SOP's protective function while limiting dissemination of original intimate files beyond the authorised custodian.²⁸

Finally, coordination should include a process for preservation beyond 180 days where proceedings require it. Rule 3(1)(g) already contemplates longer retention where required by a court or lawfully authorised government agency. The practical problem is timing. If an investigator requests preservation shortly before the ordinary period expires, the platform should have a reliable mechanism for extending the hold without altering the underlying record. A documented legal-hold procedure would protect both evidentiary integrity and compliance with deletion obligations once the authorised period ends.

A. A Model Sequence for Matched Reuploads

At the reporting stage, an affected person submits a qualifying NCII complaint through an authorised channel. The intermediary acts within the applicable Rule 3(2)(b) period and records the removal event, together with source details, complaint reference and information falling within the Rule 3(1)(g) preservation duty. Where appropriate, a detection fingerprint is registered for recurrence prevention and its purpose and algorithm are distinguished from the integrity digest of any evidentiary file. The complainant receives confirmation of the protective action and a reference usable in subsequent dealings with authorities.

At the subsequent-match stage, an intermediary encountering a candidate reupload records a fresh platform-specific instance and the grounds on which removal or disabling occurred. Its incident record links to the prevention reference while retaining independent timestamps, source-system details, account identifiers where available and the decision made about the match. Where a lawful information request follows, the responsible custodian exports the relevant retained object and event information with a verifiable integrity report and material supporting Section 63 certification. Investigators assemble the wider record across relevant custodians, while the court separately considers the weight of detection, context and attribution evidence.

Throughout retention, the original intimate material remains under restricted access with an auditable record of viewing, transmission, export and legal hold decisions. The platform records the ordinary 180-day preservation requirement and any further lawful period separately, and reviews retention after the applicable ground expires. A decision concerning continued use of a prevention fingerprint should be assessed independently from the retention

²⁸ Id. at 7–8; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(g) (India).

of the underlying intimate file, with appropriate safeguards where linked identifiers create reidentification risks. The arrangement limits additional exposure while preserving sufficient institutional accountability for a particular dissemination event.

VII. OBJECTIONS AND LIMITS OF THE PROPOSED STANDARD

The general preservation obligation may appear to render a further event specification redundant, especially for sophisticated services already operating comprehensive logging systems. The legal difficulty, however, concerns the common interpretive status of the resulting records rather than an assumption that all providers lack them. A standard that distinguishes a candidate similarity match from a platform event and a certified computer output supplies a bounded specification for existing obligations and enables meaningful scrutiny across heterogeneous services. Its administrative cost should be evaluated against the risk of either evidence loss or exaggerated inferential claims, with simplified implementation for intermediaries handling limited data.

A second concern arises from the conflict between the affected person's wish for withdrawal and the retention of highly sensitive records. The statutory framework already separates disappearance from public access from limited investigative preservation, so the appropriate legal response is strict custodial limitation and a documented review of continuing retention grounds. Notice to the complainant should identify that distinction without promising immediate destruction of every copy or disclosing information about an investigation. The proposed architecture also keeps prevention identifiers separate from full-resolution retained material, allowing independent assessment of privacy risks across those functions.

Matching systems vary in their susceptibility to transformations, false matches and missed matches, particularly where the content has been edited or synthetically generated. The proposal therefore depends neither upon universal accuracy nor upon the assumption that the 2025 SOP mandates a particular perceptual algorithm. A detection output should record its technique and review status, while the integrity digest of an evidentiary export serves a separate authentication function. Evidence of a content relationship supports only the inference warranted by that relationship, leaving identification, knowledge, consent and other elements of an alleged offence for independent proof.

A fourth objection concerns jurisdiction and data localisation. Global platforms may store records across multiple jurisdictions, and lawful disclosure can be complicated by cross-border processes. Evidentiary continuity cannot eliminate those difficulties. It can ensure that records remain preserved while appropriate legal mechanisms are used. Deletion before a

request is resolved creates an avoidable obstacle; secure retention maintains the possibility of lawful access without predetermining the jurisdictional route.

The evidence supporting this doctrinal argument is documentary. The Rules, SOP and reported decisions establish the legal obligations and the information publicly specified for their implementation, while furnishing no representative audit of internal platform preservation practice, algorithm configuration or the frequency of NCII prosecutions relying upon hash matches. Accordingly, the proposed incident standard is a legal-design inference from the public framework, rather than a demonstrated account of systematic data loss. Future investigation should examine whether actual custodial records contain the proposed fields and whether investigators and defendants obtain sufficiently interpretable exports, using research protocols that avoid collecting or reproducing intimate imagery.

VIII. CONCLUSION

India's NCII framework now combines a two-hour response to qualifying complaints with a longer investigative preservation obligation and an SOP expressly designed to detect reappearing material through shared hashes. These measures respond to different stages of abuse, yet they generate a new evidentiary demand when a prevention signal initiates removal of a distinct post or account instance. The legal content of that demand is supplied partly by Rule 3(1)(g) and partly by the source, integrity and certification requirements of the Bharatiya Sakshya Adhiniyam. Their interaction supports a standard tied to the particular event of dissemination rather than to the repeated image alone.

The proposed incident-provenance standard separates a reusable prevention fingerprint from the platform-specific record documenting each appearance and moderation action. A lawful export from the latter may support proof of posting circumstances and provide material for Section 63 certification, while the former supplies an appropriately limited account of content identity or similarity. This division follows the existing preservation duty and the Supreme Court's recognition of the importance of electronic-record custody, while addressing the more recent cross-platform prevention workflow described in the NCII SOP. It creates a workable basis for both contesting an inference from a hash match and retaining records that an affected person lacks the means to secure personally.

The distinction also gives the constitutional commitment to dignity a concrete procedural form. Rapid withdrawal minimises renewed public exposure, restricted retention preserves the possibility of accountability, and event-specific provenance limits the risk that automated similarity will be overstated as evidence of individual culpability. In an environment where

authentic, altered and synthetic sexual imagery may circulate through several services, the integrity of a legal remedy depends upon maintaining those distinctions across the institutions that detect content, document events and assess proof.

