DEEPFAKE TECHNOLOGY AND NON-CONSENSUAL DIGITAL CONTENT IN INDIA: EXAMINING CRIMINAL LIABILITY, PRIVACY RIGHTS, VICTIM PROTECTION AND THE NEED FOR COMPREHENSIVE LEGAL SAFEGUARDS

Harinath Reddy G, School of Law, Aurora Deemed to be University, Bhongir, Telangana

ABSTRACT

Deepfake abuse exposes a mismatch between the speed of digital injury and the legal processes available to contain it. An identifiable person can be placed in a fabricated intimate depiction without any original private recording, while copies can remain accessible after the first upload is removed. This article examines Indian criminal law, constitutional privacy, intermediary regulation and procedural remedies through doctrinal analysis. It incorporates the February 2026 amendments to the Information Technology Rules and distinguishes notified obligations from consultation proposals. The article argues that existing offences provide substantial but uneven coverage: obscenity provisions regulate sexual content, voyeurism provisions depend on particular factual conditions, and fraud or defamation provisions protect interests that do not fully capture sexual autonomy. Stronger platform duties improve immediate intervention but do not themselves create a comprehensive substantive offence or a complete compensation mechanism. A coherent response should expressly address authentic and fabricated intimate depictions, distinguish creation from distribution and threats, and provide accessible civil protection alongside carefully defined criminal liability. Rapid removal must operate with secure evidence preservation, proportionate identification procedures, confidential complaints and meaningful review. The proposed approach protects consent and dignity without criminalising synthetic media as a technology or allowing privacy claims to become unrestricted powers of censorship.

Keywords: Deepfakes; image-based sexual abuse; privacy; criminal liability; intermediary responsibility; victim protection.

I. Introduction

A fabricated intimate image can violate a person's autonomy even when no camera recorded the depicted event. The injury lies in attaching an unwanted sexual representation to an identifiable person and exposing that representation to others. Proving that the image is false may help rebut an allegation about conduct, but it does not necessarily end humiliation, coercion or repeated circulation. Legal analysis must therefore ask both whether an existing offence applies and whether the available remedy can stop the particular injury.

This article advances a consent-centred approach to non-consensual digital content. Its principal focus is intimate visual and audiovisual material, including altered or generated depictions. Fraudulent voice cloning and other impersonation illustrate adjacent offences, but are not treated as identical wrongs. A political parody, a deceptive financial instruction and an intimate fabrication require different legal assessments. Neither the use of artificial intelligence nor the absence of consent, taken alone, should make every representation criminal.

The analysis is doctrinal and normative. It examines statutory elements, constitutional decisions and notified intermediary rules, then develops reform proposals. It does not report interviews, conviction rates or an empirical measurement of deepfake prevalence. The regulatory discussion uses the official consolidated IT Rules updated on 10 February 2026 and their accompanying notification. The April 2026 consultation material is identified as a proposal in the source reviewed, rather than treated as proof of an enacted amendment. This source boundary matters because an advisory, a draft rule and a penal statute have different legal consequences.[1]

II. Literature and the Analytical Gap

Chesney and Citron connect deepfakes with privacy injury, democratic disruption and difficulties of accountability. Their analysis also identifies the danger that awareness of fabrication allows genuine evidence to be dismissed as fake. McGlynn and Rackley situate non-consensual creation and circulation of sexual images within image-based sexual abuse,

[1] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 10, 2026) (effective Feb. 20, 2026), https://www.meity.gov.in/static/uploads/2026/02/f55fe52418b03f58b0669f6a8bc03b6d.pdf; Ministry of Electronics & Information Technology, Notice Inviting Further Comments on Draft Amendments (Apr. 21, 2026), https://www.meity.gov.in/static/uploads/2026/04/ec197f1206279efb4964965f0dede6c1.pdf.

placing sexual autonomy and dignity at the centre. Together, these approaches explain why factual falsity and sexual exploitation overlap but are not interchangeable legal concerns.[2]

The contribution of this article is to apply that distinction to India's combination of general offences, specialised cyber provisions and the 2026 intermediary amendments. Its analytical gap concerns the relationship between these mechanisms, rather than a claim that scholarship has ignored deepfakes. A platform may be obliged to remove a prima facie abusive image even where proving a particular creator's criminal guilt requires further evidence. Equally, conviction does not automatically secure comprehensive removal, confidentiality or compensation. Evaluating those separate functions avoids treating a long list of applicable sections as a complete system of protection.

III Consent and the Nature of Digital Injury

Consent should be assessed for the act in question. Agreement to take an intimate photograph does not necessarily authorise disclosure. Permission to publish an ordinary portrait does not establish permission to generate a sexual depiction. Agreement to one audience or purpose does not automatically extend to another. Indian voyeurism legislation already recognises an important part of this distinction: consent to capture does not excuse dissemination where dissemination was not consented to.[3]

Fabrication adds another problem. A victim may never have participated in the supposed private act. Requiring an authentic underlying recording would make the availability of protection depend on the method chosen by the perpetrator. A future definition should therefore cover a depiction that represents an identifiable person as nude or engaged in specified intimate conduct, whether authentic, altered or generated. Identifiability should include contextual recognition by people who know the victim, rather than require a full name or universal public recognition.

The concept must nevertheless have boundaries. This article does not propose criminalising every unauthorised photograph, criticism, fictional portrayal or embarrassing publication. Intimacy, identifiability, the relevant act and culpability should each be defined. Legitimate

[2] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019); Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 OXFORD J. LEGAL STUD. 534 (2017).
[3] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77, expl. 2 (India).

reporting about abuse should generally describe the incident without reproducing the intimate material. Public curiosity about a person does not, by itself, justify displaying a sexual fabrication of that person.

IV Criminal Liability under Existing Indian Law

A Privacy and sexual content under the Information Technology Act

Section 66E of the Information Technology Act, 2000 addresses intentional or knowing capture, publication or transmission of an image of a person's private area without consent in circumstances violating privacy. Its maximum punishment is three years' imprisonment, a fine not exceeding two lakh rupees, or both. Its bodily focus gives it obvious relevance to authentic intimate images. Application to a wholly fabricated body attributed to another person is less straightforward because the statutory language links the image to that person's private area and circumstances of privacy. The article identifies an interpretive difficulty, not a judicially settled exclusion of every synthetic image.[4]

Sections 67 and 67A address publishing, transmitting or causing publication or transmission of specified obscene material and material containing sexually explicit acts or conduct in electronic form. Their wording is capable of engaging synthetic material; an authentic recording is not invariably necessary. A fabricated image must nevertheless satisfy the relevant content threshold. Section 67A carries, on first conviction, imprisonment up to five years and a fine up to ten lakh rupees; subsequent conviction permits imprisonment up to seven years and a fine up to ten lakh rupees.[5]

These provisions do not make obscenity and non-consent the same concept. A publication may violate sexual autonomy without fitting neatly within a statutory sexual-content threshold. Conversely, liability under a publication offence cannot simply be inferred from private creation with no publication or transmission. Investigators should identify the act proved rather than describe possession, creation, sending and publication as interchangeable. Victims who provide material through a secure complaint process must also be distinguished from people circulating it abusively.

[4] Information Technology Act, No. 21 of 2000, § 66E (India). See also Information Technology (Amendment) Act, No. 10 of 2009, § 32 (India).
[5] Information Technology Act, No. 21 of 2000, §§ 67–67A (India).

Identity misuse and commercial deception require their own analysis. Section 66C concerns dishonest or fraudulent use of another person's electronic signature, password or other unique identification feature. It is not an automatic charge whenever a face is copied. Section 66D addresses cheating by personation using a communication device or computer resource. A cloned voice used to induce a transfer may engage it if the elements of cheating and personation are established. The technological label cannot substitute for proof of dishonest conduct.[6]

B Offences under the Bharatiya Nyaya Sanhita

Section 77 of the Bharatiya Nyaya Sanhita, 2023 concerns watching or capturing a woman engaged in a private act in specified circumstances, or disseminating such an image. The section protects women as victims and now begins with the word “Whoever” for the offender. Its explanation separately addresses unauthorised dissemination after consensual capture. Where no woman actually performed the depicted act, applying the capture-based language to a fully generated scene raises a question that express legislative language would resolve more clearly.[7]

Other BNS provisions apply according to the conduct alleged. Sections 75, 78 and 79 may be relevant to sexual harassment, stalking and intrusion upon a woman's privacy, subject to their particular elements and gendered formulations. Section 351 concerns criminal intimidation, including specified threats intended to cause alarm or compel conduct. Section 308 addresses extortion and associated acts. A demand backed by a threat to release an intimate fabrication may engage these provisions, but a completed extortion charge requires its statutory conditions; the threat should not be casually equated with completed delivery of property.[8]

Sections 318 and 319 address cheating and cheating by personation. Sections 335, 336 and 340 concern false documents or electronic records, forgery and specified use of forged records. A fabricated recording may become relevant to these offences when deployed with the necessary attribution and intention. It is not correct to treat every edited video as forgery. Section 356 on defamation may address an imputation harming reputation, subject to its elements and exceptions. Reputation remains an incomplete substitute for intimate autonomy: the wrong

[6] *Id.* §§ 66C–66D.
[7] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77 (India).
[8] *Id.* §§ 75, 78–79, 308, 351.

should not depend on endorsing social prejudice against the person depicted.[9]

This overlap permits prosecution of many serious incidents but leaves uneven coverage. A person may deliberately create an identifiable adult's sexual fabrication for a targeted abusive purpose without yet distributing it, demanding money or making a conventional reputational imputation. Whether existing provisions cover that conduct must be argued from their wording. Parliament should resolve any intended extension openly, rather than leave criminal liability to expansive analogies. Applicable repeal and savings provisions must also be considered when the alleged conduct predates the new criminal codes.

C Children and responsibility for participation

Where children are depicted, section 67B of the IT Act contains a wider range of prohibited activities than adult-content publication provisions, including specified creation, collection, browsing and downloading of electronic material depicting children in an obscene, indecent or sexually explicit manner. The Protection of Children from Sexual Offences Act, 2012 additionally regulates use of children for pornographic purposes and specified storage conduct. Its definition of child pornography includes certain digitally generated images appearing to depict a child and modified images appearing to depict a child. Synthetic production therefore cannot be assumed to place child sexual abuse material outside the law.[10]

A creator, commissioning customer, knowing distributor and passive service provider occupy different positions. Abetment, conspiracy and applicable corporate-liability provisions require their own factual foundation. Supplying a general-purpose tool does not itself prove participation in a particular offence. Conversely, a person who deliberately commissions or assists an unlawful fabrication cannot necessarily avoid responsibility by pointing to the software that produced it. Liability should follow proven contribution and the required mental element.

V Privacy Rights and the Limits of Regulation

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognised privacy as a fundamental right rooted in liberty, dignity and constitutional freedoms. Its reasoning

[9] *Id.* §§ 318–319, 335–336, 340, 356.
[10] Information Technology Act, No. 21 of 2000, § 67B (India); Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 2(1)(da), 13–15 (India).

encompasses bodily and informational interests. Applied to intimate fabrication, that framework supports the argument that privacy protects meaningful control over intimate representation, not merely secrecy surrounding an authentic event. This is an application of constitutional principle to the present problem, rather than a claim that Puttaswamy itself decided a deepfake prosecution.[11]

The State's protective role must coexist with constitutional limits on its own measures. A system that requires every complainant to deposit unnecessary identity documents or intimate files in widely accessible databases could reproduce the exposure it seeks to prevent. Identity verification should use the minimum necessary information, with access controls, retention limits and accountable disclosure. Protection should also be available without celebrity status or commercial value in a person's likeness.

Article 19(1)(a) and the grounds in Article 19(2) constrain restrictions on expression. Shreya Singhal v. Union of India invalidated section 66A and read down the actual-knowledge standard under section 79(3)(b) in relation to intermediary takedowns. Section 66A must not be presented as an available deepfake offence. The judgment's treatment of vagueness explains why a prohibition of all “offensive” or “misleading” synthetic expression would be constitutionally vulnerable.[12]

Protection of sexual autonomy should therefore be expressed through precise elements and proportionate remedies. Clearly contextualised parody, consensual creative work and public-interest investigation cannot be placed in the same category as targeted intimate abuse. At the same time, attaching a “parody” label should not automatically excuse an identifiable person's sexual exploitation. Courts must examine substance, context and necessity rather than allow either the label “AI” or the label “satire” to decide the case.

VI Intermediary Duties after the February 2026 Amendments

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 were notified through G.S.R. 120(E) on 10 February 2026 and came into force on 20 February 2026. They introduce a definition of synthetically generated

[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–98, 325 (India) (opinion of Chandrachud, J.).
[12] INDIA CONST. art. 19; *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 87–90, 117, 119 (India).

information covering specified realistic audio, visual and audiovisual representations, while excluding certain routine or good-faith uses. Rule 3(3) imposes technical due-diligence obligations relating to unlawful synthetic information and labelling and provenance requirements for other covered synthetic information. Rule 4(1A) introduces declaration, verification and labelling duties for significant social media intermediaries.[13]

The complaint deadlines must be distinguished. Under amended rule 3(2)(b), an intermediary must, within two hours of receiving a qualifying complaint from the individual or someone acting on that individual's behalf, take all reasonable and practicable measures to remove or disable access to the specified prima facie intimate or impersonation content, including artificially morphed images. This is the direct victim-complaint route. Under rule 3(1)(d), the separate period is three hours after actual knowledge arising through the prescribed court order or reasoned governmental intimation. Neither period should be confused with the general grievance-resolution timetable.[14]

These changes make descriptions of a universal twenty-four-hour NCII takedown rule outdated for the notified February framework. They also strengthen the case for accessible complaints: a short deadline is useful only when a victim can reach the appropriate officer and identify the content without unreasonable procedural demands. Rule 3(1)(g) requires preservation of removed information and associated records for 180 days, or a longer lawfully required period. Removal from public access and preservation for investigation are therefore compatible functions.[15]

Labelling addresses authenticity, not consent. A prominent notice that an intimate image is fabricated does not undo its unauthorised sexual use. Nor does a failure of due diligence itself establish every element of a criminal offence. Section 79 provides conditional protection for qualifying intermediary activity; losing that protection exposes the provider to assessment under otherwise applicable law. The analysis must still establish the legal basis for liability. A provider's own creation or active participation also needs to be separated from its role as a host

[13] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 2(1)(wa), 3(3), 4(1A), as amended by G.S.R. 120(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 10, 2026) (India). Official consolidated text: https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf.

[14] *Id.* rr. 3(1)(d), 3(2)(a)–(b). The February amendments replace twenty-four hours with two hours in rule 3(2)(b) and thirty-six hours with three hours in rule 3(1)(d).

[15] *Id.* r. 3(1)(g).

of third-party content.[16]

The April 2026 notice reviewed for this article sought comments on additional changes, including continuous visual labelling. A consultation notice does not prove that its proposal was subsequently enacted. More fundamentally, subordinate rules cannot resolve every uncertainty in the wording of primary criminal legislation. Their operation must remain consistent with the parent Act and constitutional requirements. Effective victim protection consequently needs substantive rights and remedies alongside platform compliance.[17]

VII Victim Protection and Access to Effective Remedies

A Complaints and immediate relief

Criminal reporting and content removal should proceed on separate but coordinated tracks. BNSS section 173 permits information about a cognizable offence irrespective of the area where it occurred, including by electronic communication subject to signature within three days. It provides additional recording safeguards for specified offences against women. A platform complaint should not be made dependent on a final criminal judgment, since rule 3(2)(b) addresses prima facie content and immediate containment.[18]

Civil proceedings may seek interim restraint, removal or de-indexing and appropriate final relief. Courts should identify the content and persons affected precisely enough to permit implementation while protecting lawful material. In Mrs X v. Union of India, the Delhi High Court rejected an approach that made a victim repeatedly identify every duplicate URL and discussed targeted measures against reported non-consensual intimate imagery. Its reasoning supports reducing repetitive burdens, while its attention to the dangers of broad filtering cautions against treating every privacy complaint as a mandate for indiscriminate monitoring.[19]

De-indexing reduces discoverability but does not necessarily delete the source. Removal by

[16] Information Technology Act, No. 21 of 2000, § 79 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 2(1B), 7 (India), as amended in 2026.
[17] Ministry of Electronics & Information Technology, *supra* note 1. The notice records a consultation proposal; the article does not infer enactment from that document.
[18] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 173(1)–(2) (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b) (India), as amended in 2026.
[19] *Mrs X v. Union of India*, W.P. (Crl.) 1505/2021, 2023:DHC:2806, ¶¶ 52–56 (Delhi H.C. Apr. 26, 2023) (India), https://indiankanoon.org/doc/105980506/. The discussion concerns the reasoning of this decision, not a claim that every form of proactive filtering is universally mandated.

one host does not eliminate copies elsewhere. An effective order should therefore specify whether it concerns hosting, search results, identified duplicates or preservation. It should include a practical escalation channel for recurrence. These distinctions also help courts assess compliance fairly: a platform should account for the measures within its control without promising an impossible erasure of every copy on the internet.

B Evidence and confidential participation

Electronic admissibility and factual authenticity are distinct questions. The Bharatiya Sakshya Adhiniyam, 2023 addresses electronic records in sections 61 to 63 and contains a prescribed certificate framework. Compliance with an applicable evidentiary requirement does not establish that the depicted event occurred or identify who fabricated it. Investigators should preserve source files where lawfully available, account identifiers, timestamps, communication records and relevant device information, and document collection and transfer. Expert examination should explain its method and limitations rather than rely on an unexplained authenticity score.[20]

Preservation must avoid multiplying exposure. Controlled access to exhibits, redaction in public filings and appropriate confidential handling should accompany forensic work. The victim should not have to circulate the image to numerous officials merely to obtain attention. For children, POCSO imposes particular confidentiality and child-sensitive procedures. Extending comparable procedural protection to adult victims of intimate digital abuse would require clear statutory provision and implementation, rather than an assumption that every safeguard for other sexual offences already applies.[21]

Compensation requires equal attention. BNSS section 396 provides a victim-compensation framework administered through legal services authorities and state schemes, subject to applicable conditions. It does not guarantee a fixed payment for every deepfake complaint. An express scheme for intimate digital abuse should consider counselling, urgent legal assistance, reasonable removal expenses and demonstrated economic injury. Access to support should not depend entirely on identifying an anonymous perpetrator or obtaining a conviction.[22]

[20] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 39, 57, 61–63 & sched. (India).
[21] Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 23–24, 33(7), 37 (India).
[22] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 396 (India).

VIII Data Protection and Remaining Structural Gaps

The Digital Personal Data Protection Act, 2023 is relevant to identifiable photographs, voice data and processing used in generating or distributing representations. Its commencement must be described accurately. G.S.R. 843(E), dated 13 November 2025, phases commencement, placing core processing duties and individual-rights provisions in the eighteen-month category. Under that notified schedule, those provisions should not be described as fully operational remedies in October 2026. The discussion here concerns the enacted design and that commencement framework.[23]

Even when operative, the Act will not replace a dedicated intimate-abuse remedy. Section 3 contains exclusions, including certain personal or domestic processing and personal data made publicly available by the data principal or by another person under a legal obligation. A publicly posted portrait and a newly fabricated intimate depiction require distinct analysis; an exclusion for source data does not settle the legality of every later output. The Act's penalty structure also does not supply a general compensatory award to each victim. These limits reinforce the need for civil relief independent of a data-regulatory complaint.[24]

Three structural difficulties remain. Offences protect different interests and sometimes different classes of victims. Platform mechanisms can contain content without resolving compensation or attribution. Cross-border conduct introduces enforcement obstacles even where a statute asserts extraterritorial reach. A reform programme should address each problem directly, rather than assume that expanding territorial language or increasing sentences will produce practical access to justice.

IX A Coherent Framework for Reform

Parliament should expressly define non-consensual intimate depiction to include authentic and synthetic visual or audiovisual material representing an identifiable person. A complementary provision should address intimate audio impersonation where clearly specified. The definition should focus on specified intimate content and lack of consent to the relevant act. Gender-

[23] Digital Personal Data Protection Act, No. 22 of 2023, § 1(2) (India); Notification, G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025) (India), https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf.

[24] Digital Personal Data Protection Act, No. 22 of 2023, §§ 3, 12, 33–34 (India). Section 34 directs statutory penalties to the Consolidated Fund of India. The commencement qualification in the preceding paragraph applies to the provisions discussed here.

neutral protection would avoid leaving adults outside the central remedy while allowing child-specific offences and safeguards to remain stronger.

Creation, disclosure and threats should be addressed separately. A disclosure offence should require intentional dissemination with knowledge of, or clearly defined recklessness concerning, non-consent. A creation offence should contain additional culpability, such as knowledge of non-consent combined with an intention to distribute, coerce or seriously harass, rather than criminalise undefined private thought or every synthetic experiment. Threats should be actionable when used to coerce or cause legally specified harm even if the threatened file has not yet been produced. These are proposed elements, not a description of an existing unified offence.

Consent should be voluntary, specific and tied to purpose and audience. Prior relationships, public photographs, silence and consent to capture should not automatically establish consent to distribution. The prosecution should retain the burden of proving the offence; a complainant's inability to produce a written refusal cannot substitute for that burden or defeat a complaint automatically. Narrow exceptions should cover genuinely necessary legal proceedings, evidence preservation and public-interest uses, subject to safeguards against gratuitous disclosure.

A parallel civil remedy should permit urgent interim orders without waiting for conviction. It should provide confidential filing, proportionate identification of unknown defendants, compensation and precisely framed directions against identified material and verified duplicates. Emergency orders should receive prompt subsequent review, with reasons and an opportunity to contest them. A person whose lawful material is wrongly removed needs an accessible correction process; appeals should not automatically restore apparently abusive intimate material before review.

Platform enforcement should build on the February 2026 duties through practical standards for multilingual complaints, authorised representatives, trained review and secure preservation. Repeat-upload controls should be targeted at confirmed abusive material, audited for erroneous matches and subject to contextual human review. Identity disclosures should follow lawful process. Transparency reporting should measure response times, recurrence and successful appeals without revealing victims' identities or reproducing the material.

Finally, implementation requires funded forensic capacity, legal aid and support independent of prosecution. A coordinating service could help route one complaint to relevant platforms and investigators while retaining only necessary data. Its success should be measured by containment, victim access and fair decisions, as well as case outcomes. International cooperation should improve lawful preservation and evidence requests without abandoning procedural safeguards. A comprehensive framework can be created through coordinated amendments and remedies; it need not depend on a single omnibus statute.

X Conclusion

Indian law already supplies meaningful tools against many forms of deepfake abuse, and the February 2026 intermediary amendments materially strengthen the regulatory response. The remaining problem is uneven substantive coverage and fragmented relief. Consent, intimate autonomy and identifiability provide a sound basis for a more coherent framework. Precisely defined offences should operate alongside rapid civil protection, confidential procedures, secure evidence preservation and accessible compensation. That combination addresses the victim's continuing injury while preserving the constitutional limits that make digital regulation legitimate.