INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"RETHINKING SECTIONS 43 AND 66 OF THE INFORMATION TECHNOLOGY ACT: THE NEED FOR A STATUTORY SAFE HARBOUR FOR GOOD-FAITH SECURITY RESEARCH"

AUTHORED BY - VEENAVARDHANI S
B.B.A., LL.B(Hons), SCHOOL OF LAW
SASTRA DEEMED TO BE UNIVERSITY, Thanjavur, Tamil Nadu

The Information Technology Act, 2000 criminalizes unauthorized access to computer systems under Sections 43 and 66, yet neither provision distinguishes between malicious intrusion and good-faith cybersecurity research. Section 43 imposes civil liability for unauthorized access irrespective of intent, while Section 66 converts specified acts into criminal offences only where committed dishonestly or fraudulently — a mens rea requirement that nonetheless leaves the boundary between legitimate security testing and criminal conduct undefined in statute. Although the Indian Computer Emergency Response Team (CERT-In) operates a Responsible Vulnerability Disclosure and Coordination Policy encouraging researchers to report security flaws, the policy expressly disclaims providing any exemption from applicable law, leaving disclosers fully exposed to civil and potential criminal liability for the very conduct the policy solicits. This paper examines whether India's existing statutory and policy framework adequately protects good-faith security researchers, and argues that the absence of an express statutory safe harbour — despite civil society advocacy, including representations by the Internet Freedom Foundation — creates a chilling effect that may discourage responsible disclosure in favour of non-disclosure or grey-market exploitation of vulnerabilities. Section 79 of the IT Act already demonstrates that Parliament has legislatively accepted the principle of conditional immunity, having extended it to intermediaries; this paper argues that the same logic, subject to appropriately tailored conditions, should be extended to good-faith security researchers under Sections 43 and 66. Drawing on comparative approaches, including reform debates surrounding the U.S. Computer Fraud and Abuse Act and coordinated vulnerability disclosure obligations under the European Union's Cyber Resilience Act, the paper proposes a conditional statutory safe harbour for India — limited to good-faith purpose, minimal necessary testing, no data exfiltration or persistence, and prompt, coordinated disclosure — as a

ISSN: 2582-6433

legislative amendment to the IT Act. In doing so, the paper contributes a doctrinal analysis to an area largely unaddressed in Indian legal scholarship, situating cybersecurity policy and criminal law within a coherent statutory framework rather than leaving their present tension unresolved.

Keywords: Information Technology Act; cybersecurity research; coordinated vulnerability disclosure; safe harbour; Section 43; Section 66; Section 79; CERT-In; Computer Fraud and Abuse Act; Cyber Resilience Act

1.Background, Introduction and Significance of Study

1.1 Background

Security researchers can't find a flaw in a system unless they do something to the system that the owner has not expressly allowed them to do. Therefore, the technical act of a researcher and an attacker could be identical. The difference is that the researcher wants the flaw corrected and the attacker wants to profit from it (Kerr 2003)[1]. A proper legal regime must be able to distinguish between the two.

The IT Act does not do so. Section 43 Any person who, without the permission of the owner or person in charge of a computer, computer system or computer network, accesses or downloads or copies any data, introduces a virus or contaminant, disrupts or denies service or alters or destroys information, is liable to pay compensation[2]. There is no need for dishonesty, malice or negligence; the lack of permission suffices. Section 66 makes the same acts an offense punishable with a punishment of up to three years' imprisonment, or with a fine of up to five lakh rupees or both, but only if done "dishonestly or fraudulently"[3]. The Explanation to Section 66 refers the meanings of those words to Sections 24 and 25 of the Indian Penal Code, 1860[4], now brought into Section 2(7) and Section 2(9) of the Bharatiya Nyaya Sanhita, 2023[5].

1.2 Introduction

The Indian Computer Emergency Response Team (CERT-In), the national agency established under Section 70B of the Act, published its Responsible Vulnerability Disclosure and Coordination Policy on 3 September 2021[6]. The policy explains where to report, what a report

[1] Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes *78 New York University Law Review 1596 (2003).*
[2] Information Technology Act,2000; section 43(a) to 43 (j)
[3] Section 66 of Information Technology Act, 2000.
[4] Sections 24 and 25 of the Indian Penal Code, 1860.
[5] Section 2(7) and Section 2(9) of the Bharatiya Nyaya Sanhita, 2023
[6] Indian Computer Emergency Response Team (CERT-In)

ISSN: 2582-6433

should include and how CERT-In will coordinate a fix. However, Clause 7 states that reporting does not relieve the discloser from compliance and that the discloser is still responsible for what they did to find the flaw (IFF 2021a[7]). The Internet Freedom Foundation (IFF) opposed. CERT-In responded that its policy is an executive instrument and has to operate within the existing law. IFF then requested the Ministry of Electronics and Information Technology[8] (MeitY) to amend the IT Act to protect genuine researchers (IFF 2021b[9]).

That trade-off highlights the problem. And the agency requesting disclosures states it cannot protect those who provide them – and the only body that can, Parliament, has not acted. This paper tries to fill this gap and suggests how to do so.

1.3 Significance of the chosen Research Area

The topic matters for five reasons.

1. Security: India has a large and growing digital public infrastructure. The IFF (2020) has warned that discouraging domestic researchers makes the country dependent on foreign researchers who are not accountable to Indian courts.[10]
2. Econometrics: The literature shows that the results of disclosure depend on the incentives and the channels that researchers have[11]. The discloser assumes the entire cost of legal risk.
3. Legal consistency: There is already one conditional immunity under the IT Act (Section 79). It is as much a matter of consistency as of applying the technique to a second public-interest activity.
4. Timeliness: The United States has adopted a prosecutorial policy for good faith research (DOJ 2022)[12]. The European Union's Cyber Resilience Act, Regulation (EU) 2024/2847[13], has required manufacturers to report actively exploited vulnerabilities since 11 September 2026 (Hogan Lovells 2026)[14]. India's framework has not changed.
5. Scholarly gap: The research are mostly found on plenty of discussion around Section 66A and intermediary liability, but very little doctrinal papers on researcher liability under Sections 43 and 66.

[7] Internet Freedom Foundation (2021a).
[8] Ministry of Electronics and Information Technology, 2016
[9] Internet Freedom Foundation (2021b). MeitY
[10] Strickland, Lea. "The Rise of Foreign Influence and Risks in Government-Funded Research." *SBIR BASICS*, 13 May 2026, https://sbirbasics.com/2026/05/the-rise-of-foreign-influence-and-risks-in-government-funded-research/.
[11] Arora, A., Telang, R. and Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science*, 54(4), 642–656
[12] Department of Justice 2022
[13] Regulation (EU) 2024/2847 (Cyber Resilience Act)
[14] Hogan Lovells (2026). EU Cyber Resilience Act: Preparing for vulnerability and incident reporting

ISSN: 2582-6433

2. Literature Review

2.1 What does "Authorization" mean?

Kerr 2003 is the foundational study of the unauthorized-access statutes. He notes that legislatures have added "access" and "authorization" to computer crime laws without defining them, that courts have interpreted them inconsistently, and that some rulings consider any breach of a contract or terms of use as making access unauthorized[15]. He argues that the offense should be confined to bypassing code-based restrictions. This is consistent with the logic of consent in the criminal law. This is exactly the concern he raises about the vague language of authorization criminalizing innocent activity, as the phrase "without permission" in Section 43 is also not defined by the IT Act.

The U.S. Supreme Court later took a similarly narrow view. In Van Buren v. United States[16] it ruled that a person "exceeds authorized access" under the Computer Fraud and Abuse Act only by entering parts of a system off-limits to them, a "gates-up-or-down" test, not misusing information they were entitled to see. The ruling limited the statute but did not grant researchers an affirmative defense.

2.2 The economics of vulnerability disclosure

Four management and information-systems journal articles model or measure disclosure workings. Arora, Telang and Xu[17] (2008) develop a model in which a social planner chooses a protected period before disclosure, and a vendor chooses when to patch. They find that vendors tend to patch slower than is socially optimal, so the disclosure window can be used to pressure them to act faster. This is the analytical foundation for the coordinated-disclosure deadlines to which policies like CERT-EU's 90-day norm apply (CERT-EU n.d.[18]).

Kannan and Telang (2005) compare a passive CERT-type body and a for-profit market intermediary that pays for vulnerability reports[19]. They conclude that an unregulated market will tend to do worse than a CERT type mechanism, since the intermediary has an incentive to leak information. Ransbotham, Mitra and Ramsey (2012) take a more favorable view of market-based disclosure, examining two years of alert data[20]. Market-based disclosure seems

[15] Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes *78 New York University Law Review 1596 (2003).*
[16] Van Buren v. United States 593 U.S. 374 (2021)
[17] Arora, A., Telang, R. and Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science*, 54(4), 642–656
[18] CERT-EU (n.d.)
[19] Kannan, K. and Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science*, 51(5), 726–740
[20] Ransbotham, S., Mitra, S. and Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, 36(1), 43–64.

ISSN: 2582-6433

to slow down the spread of exploits, and reduce exploitation attempts. But the two studies disagree on markets, and agree that the design of the disclosure channel determines security outcomes.

Maillart et al. (2017) empirically analyze bug bounty programs[21]. They find that each researcher can expect to find only a bounded number of bugs in a given program. Programs benefit from large crowds. Organizing smoother, more predictable transactions would reduce the researchers' incentive to sell on the black market. These studies view the choice of the researcher as driven by money, vendor behavior and market design. None of these studies treat the legal exposure as a variable, although Maillart et al. (2001) implicitly recognize the black market as a competing outlet. This paper adds that variable.

2.3 Safe harbour proposals and the DOJ policy

Etcovitch and van der Merwe (2018) propose a statutory safe harbour from the CFAA and DMCA §1201 for researchers who follow a structured responsible-disclosure process[22]. Their model provides a legal guaranty for procedural compliance, the same deal this paper suggests for India.

The U.S. Department of Justice issued a limited version in May 2022 telling prosecutors not to bring charges for good-faith security research, defined as access only to test, investigate or fix a flaw, to prevent harm, with the results primarily used to further security. But two weaknesses are noted in law-firm analysis: The word "solely" leaves room to prosecute research with mixed motives, and a policy can be reversed by a future administration, unlike a statute.

2.4 Indian scenario

Sources from India are largely policy documents and advocacy[23]. IFF (2020) argues that Section 43 makes no distinction between malicious hackers and ethical researchers, as demonstrated in a 2020 post by IFF of a company threatening to sue a researcher reporting a data exposure[24]. The dispute over Clause 7 is recorded in the IFF's 2021 representations (IFF 2021a, 2021b). The Supreme Court decision in Shreya Singhal v Union of India (2015) is relevant for another reason[25]. The interpretation of Section 79 was such that the intermediaries lose immunity only in the event of a court order or a notification by the government, reflecting

[21] Maillart, T., Zhao, M., Grossklags, J. and Chuang, J. (2017)
[22] Etcovitch, D. and van der Merwe, T. (2018). *Coming in from the Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers*. Berkman Klein Center Research Publication No. 2018-4 (Harvard).
[23] *India's Cybersecurity Policy Frameworks: Key Strategies and Initiatives | RSM India*. 10 Jan. 2025.
[24] "Security Researchers Need Legislative Protection from Vexatious Lawsuits." *Internet Freedom Foundation (IFF)*, 15 Jan. 2020,
[25] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1

ISSN: 2582-6433

the judicial acceptance of conditional immunity when the conditions are clear.[26]

3. Statement of the Research Problem

Section 43 creates a civil tort of unauthorized access, whether or not with intent. Section 66 requires dishonesty or fraud but the protection it provides is a defense that can only be argued at trial, after a complaint, a FIR and possibly an arrest. It does nothing to address the liability under Section 43. CERT-In is requesting researchers to disclose, but there is no protection. The rational researcher is thus at no less legal risk on the disclosure path than on the non-disclosure or sale paths, and arguably at more.

The research problem is that India's statutory and policy framework does not differentiate between good-faith security research and unauthorized intrusion, creating a legal disincentive to responsible disclosure that executive policy cannot remove and that Parliament has not addressed.

4. Research Objectives

The aim of the study is:

1. To examine the relevance of Sections 43 and 66 of the IT Act to good-faith security testing and why the mens rea requirement of Section 66 is an inadequate safeguard.
2. To study the legal implications and scope of the CERT-In disclosure policy especially of Clause 7.
3. To explain, using the disclosure literature, how legal exposure shapes researchers' choices among coordinated disclosure, non-disclosure and sale.
4. To evaluate Section 79 as a legislative precedent for conditional immunity.
5. To propose a statutory safe harbour with conditions, institutional design and illustrative text

5. Research Questions

1. Is a good faith researcher protected in practice by the Section 66 "dishonestly or fraudulently" requirement considering that intent is only tested after the process has begun and what is left unprotected under Section 43?

[26] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

ISSN: 2582-6433

2. Why does the CERT-In policy not claim exemption, leaving the legal position unchanged? What does this tell us about the limits of executive instruments in a field governed by statute?
3. How does a researcher weigh legal risk against reward when choosing between coordinated disclosure, non-disclosure and sale, and does the present framework tilt that choice away from disclosure?
4. Is Section 79 a principled model for conditional immunity, and where do the passive conduct of intermediaries and the active conduct of researchers diverge?
5. What do the CFAA experience, the DOJ policy and the Cyber Resilience Act show about drafting and administering protection for researchers?
6. Which conditions and institutional arrangements would make an Indian safe harbour administrable, constitutional and resistant to pretextual use?

6. Scope and Limitation of the Study

The study considers sections 43 and 66 of the IT Act, 2000 as applicable to good-faith security research; CERT-In policy of 2021 and Section 70B; Section 79 and Shreya Singhal as a comparator; and, comparatively, the U.S. CFAA with 2022 DOJ policy and the EU Cyber Resilience Act. It suggests an amendment to the IT Act rather than a new standalone law.

Limitations

1. No primary empirical data: The paper does not survey/interview researchers. Claims of the chilling effect are based on doctrine, the disclosure literature and documented advocacy, not measured behavior.
2. Enforcement practice is inferred from the anecdotal press and advocacy sources.
3. The analysis is confined to two jurisdictions. The U.S. DOJ policy and the EU regulation are geared toward different problems and are juxtaposed functionally rather than equivalently.

7. Research Method:

The Statutory Architecture

Section 43: Liability is based on the absence of consent, not on motive, and is therefore more of a trespass rule than a tort based on fault. “Permission” is not defined. The text provides no answer to the question of whether a person who tests a public-facing web application, without an invitation, and without exceeding what any member of the public could reach, acts “without

ISSN: 2582-6433

permission". Kerr (2003)[27] warning of undefined authorization applies squarely here.

Section 66: The mens rea requirement appears to be a protective one, in that a researcher who intends neither wrongful gain nor wrongful loss nor deceit is outside the offense. Three problems constrain that comfort.

1. Timing: Intent is established at the trial but the costs of a complaint, FIR and possible arrest are incurred earlier. The defense is something at the end of the process, not at the beginning. There is no need for a prior judicial finding on intent for registration of a cognizable offense[28].
2. "Wrongful gain" and "wrongful loss" are not limited to money. The complainant could argue that publicity for the researcher or embarrassment and remediation cost to the owner falls within those terms. That is an interpretive risk, not a settled matter of law, and it is the kind of uncertainty that a researcher must price in.
3. A favorable reading of Section 66 does not touch Section 43. An owner can sue for compensation regardless of how pure the motive. Section 66 therefore represents at most half the exposure.

The CERT-In Policy:

CERT-In is there under Section 70B for coordination of cybersecurity functions and its disclosure policy is a useful operational channel." However, a statutory body cannot, as a matter of policy, qualify a civil remedy or criminal offense created by Parliament. And CERT-In said as much in response to IFF (IFF 2021b) and Clause 7 makes the point in terms (IFF 2021a). The result is an asymmetry: the state asks for a behavior which the same state leaves exposed. A researcher who follows the policy has no defense that they would not have had anyway.

The Chilling effect on disclosure

A researcher who discovers a vulnerability has three general options: disclose via a coordinated channel; disclose publicly without coordination; or stay quiet, either by discarding the finding, selling it, or holding it for future use. Disclosure design matters to social outcomes (Arora, Telang and Xu 2008), markets and channels influence exploitation (Kannan and Telang 2005, Ransbotham, Mitra and Ramsey 2012) and more predictable disclosure transactions lower the pull of the black market (Maillart et al. 2017).

In this context the Indian stance has a perverse aspect. The first access is just as exposed regardless of what the researcher does next, so there is no additional legal cost to remaining

[27] Kerr, O. S. (2003). Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. *New York University Law Review*, 78(5), 1596.
[28] BNSS 2023, sec. 173 replacing CrPC sec.154

ISSN: 2582-6433

silent but disclosure adds a record of the researcher having had access. Disclosure is therefore the path of greatest marginal legal risk. That is an inference from incentives and from the cases on record, not a measured outcome, and the paper treats it as such.

Section 79 as precedent

The replaced section 79 of 2008 provides immunity to intermediaries for 3rd party content, subject to a set of criteria: passive role, no initiation / modification of transmissions, due diligence. Shreya Singhal read down the knowledge trigger to the effect that immunity is lost only after a court order or a government notification and struck down Section 66A for vagueness. The lesson is: Parliament accepts conditional immunity as a technique, and the Court accepts it when the conditions are clear and checkable. Intermediaries passive carriers, researchers active probes. That is a reason for tighter conditions than the conditions of Section 79, not a reason to reject the technique**.**

Comparative Study

United States: Years of litigation followed the CFAA's phrases "without authorization" and "exceeds authorized access," (Kerr 2003), which Van Buren narrowed with its gates test. The DOJ policy of 2022 then shields good faith research from federal prosecution, defined by purpose, harm avoidance, and use of results (DOJ 2022). Its weaknesses are that it is only a policy, that 'solely' invites arguments over mixed motives, and that civil claims remain (WSGR 2022)[29].

European Union: The Cyber Resilience Act imposes responsibilities on manufacturers, who are obliged to report actively exploited vulnerabilities and serious incidents under Article 14 and the whole regime, including a coordinated vulnerability disclosure policy in Annex I, Part II (Hogan Lovells 2026; Regulation (EU) 2024/2847), is applicable from the 11th of December 2027. The Act strengthens the receiving end of disclosure. It does not itself protect the researcher who discloses.

First, not defining the authorization boundary is costly. Second, a purpose-and-conduct test for good-faith research is possible and can be embedded in a statute, rather than a revisable policy. Third, researcher protection and owner obligations are two sides of the same coin. The four conditions in Part 9 are based on the DOJ formula and include a no-persistence rule and a specified disclosure window.

[29] Wilson Sonsini Goodrich & Rosati (2022).

ISSN: 2582-6433

8. Future Directions and Recommendations

8.1. Statutory safe harbour inside the IT Act

The safe harbor should be inserted in the IT Act itself, for example as a new Section 43B or as an Explanation to Sections 43 and 66 and not in delegated legislation or policy. A statute binds courts and prosecutors alone; it is a special provision superseding the general rule (special provision test); it outlives changes of government (durability test) It should apply both to civil liability under Section 43 and criminal liability under Section 66, as protection from just one would mirror the current asymmetry.

Protection should depend on four cumulative conditions:

Good-faith purpose: The primary intent is to find, investigate or confirm a security vulnerability, and not to obtain data for private use, gain or sale.

Minimal necessary testing: Testing and any data touched are limited to what is needed to demonstrate and report the flaw.

No exfiltration or persistence: The researcher does not hold, publish or utilize data beyond that necessity. The researcher creates no backdoor or continuing access. This is the bright line, in the spirit of the gates test

Prompt, coordinated disclosure: The researcher reports to the system owner or CERT-In in a prescribed period and withholds technical details till remediation or end of prescribed window. Practice elsewhere, such as CERT-EU's 90 days extendable for good reason (CERT-EU n.d.), is a reference point and not a legal standard; CERT-In should set the window by rules.

8.2 Illustrative Statutory text

43B. Notwithstanding anything in section 43 or section 66, no person shall be liable to pay compensation under section 43, and no act shall be punishable under section 66, where the person establishes that the act was done (a) solely for the good-faith purpose of identifying, investigating or verifying a security vulnerability in a computer, computer system or computer network; (b) in a manner and to an extent no greater than reasonably necessary for that purpose; (c) without exfiltration, retention, publication or use of data beyond what was reasonably necessary to demonstrate and report the vulnerability, and without creating or keeping persistent unauthorised access; and (d) with prompt disclosure to the person in charge of the system or to the Indian Computer Emergency Response Team, within the prescribed period and manner, and without public disclosure of technical details before remediation or expiry of the prescribed period, whichever is earlier.

ISSN: 2582-6433

Explanation. The Indian Computer Emergency Response Team may, on application, determine whether clauses (a) to (d) are satisfied, and the determination shall raise a rebuttable presumption in favour of the applicant in any proceeding under section 43 or section 66.

8.3 Institutional design and interim measures

CERT-In has the technical expertise and the disclosure channel and is the natural body to make determinations on application. A determination should create a rebuttable presumption with the burden of rebutting the presumption being on an owner or a prosecutor. The safe harbor should be prospective upon conditions being met and should not require pre-authorisation, which would replicate the bug bounty model and exclude the researcher who discovers a flaw outside any engagement.

- CERT-In should modify Clause 7 so as to at least indicate that adherence to the policy will be regarded as proof of good faith, even if it does not grant immunity.
- The leadership of MeitY and the state police should produce some guidance stating that complaints made against people who reported via CERT-In should be screened before an arrest is carried out.
- Governments should draw up their own vulnerability disclosure policies, as the IFF has recommended (IFF 2021b).

They are weaker than statutes, as the experience of the DOJ has shown, and must be regarded as a temporary measure only.

8.4 Companion Reforms

India ought to adopt a duty similar to that of a CRA requiring manufacturers and operators of critical systems to keep open a disclosure channel and to respond within specified time frames. Although this matter falls within the domain of product and infrastructure regulation and is therefore outside the scope of this paper, it would bring the system to completion. The statutory references to the IPC and CrPC should also be brought up to date to refer to the BNS and BNSS.

8.5 Anticipated objections

A pretext is involved here since wrongdoers might say that they are carrying out research. The combined conditions deal with this situation: if an actor retains data, keeps access to it or delays revealing it in order to obtain payment, then that actor breaches both clauses (c) and (d) regardless of the name given to the activity.

Demonstrating the purpose: It is difficult to show what the purpose was after the fact. This difficulty is already provided for in Section 66's provision regarding 'dishonestly or fraudulently'. The use of objective proxies (such as proportionate testing, no retention, and

ISSN: 2582-6433

timely reporting) makes the investigation easier, and a determination by CERT-In takes the initial assessment to a specialist.

Issues relating to the Constitution and the federal structure: since the IT Act is legislation at the Union level and criminal law is included in the Concurrent List, Parliament has the authority to amend sections 43 and 66. The objection on grounds of vagueness under Article 14 is dealt with by clearly setting out the conditions, and the present situation is more vague. The case of Shreya Singhal demonstrates the Court's willingness to grant conditional immunity.

9. Conclusion

India is asking researchers to identify and report any flaws while offering them no legal protection for the testing needed to do so. Section 43 does not take into account the researcher's motive, the intent test in Section 66 serves as a defence at the end of the process, and CERT-In's policy also denies any protection. Conditional immunity has already been used by Parliament under Section 79, and both the United States and the European Union demonstrate that definitions based on purpose and conduct are feasible and that policy-level protection is vulnerable. A narrow safe harbour, based on four conditions and with CERT-In's determinations carrying a rebuttable presumption, would give the law a clear distinction between a researcher and an intruder. It would not eliminate the criminality of unauthorized access in general nor would it weaken the remedies available against actual intrusion.

Reference

1. Arora, A., Telang, R. and Xu, H. (2008). *Management Science*, 54(4), 642–656. https://doi.org/10.1287/mnsc.1070.0771z
2. Etcovitch, D. and van der Merwe, T. (2018). *Coming in from the Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers*. Berkman Klein Center Research Publication No. 2018-4 (Harvard). https://dash.harvard.edu/entities/publication/73120379-406a-6bd4-e053-0100007fdf3b
3. Kannan, K. and Telang, R. (2005). Market for software vulnerabilities? *Management Science*, 51(5), 726–740. https://doi.org/10.1287/mnsc.1040.0357
4. Kerr, O. S. (2003). Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. *New York University Law Review*, 78(5), 1596.

ISSN: 2582-6433

https://nyulawreview.org/issues/volume-78-number-5/cybercrimes-scope-interpreting-access-and-authorization-in-computer-misuse-statutes/

5. Maillart, T., Zhao, M., Grossklags, J. and Chuang, J. (2017). *Journal of Cybersecurity*, 3(2), 81–90. https://arxiv.org/abs/1608.03445
6. Ransbotham, S., Mitra, S. and Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, 36(1), 43–64. https://aisel.aisnet.org/misq/vol36/iss1/6

Cases, statutes and official instruments

7. *Van Buren v. United States*, 593 U.S. 374 (2021). https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf
8. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1. https://indiankanoon.org/doc/110813550/
9. *Sharat Babu Digumarti v. Government of NCT of Delhi*, (2017) 2 SCC 18.
10. Information Technology Act, 2000, sec 2, sec 43, sec 66, sec 70B, sec 79 (as amended 2008). India Code, https://www.indiacode.nic.in
11. Bharatiya Nyaya Sanhita, 2023, sec 2(7), sec 2(9); Bharatiya Nagarik Suraksha Sanhita, 2023, sec 173. India Code, https://www.indiacode.nic.in
12. Regulation (EU) 2024/2847 (Cyber Resilience Act). https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
13. U.S. Department of Justice (2022). *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act*, 19 May 2022. https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act
14. CERT-EU (n.d.). https://cert.europa.eu/responsible-disclosure-policy

Policy, advocacy and commentary

15. Internet Freedom Foundation (2020). https://internetfreedom.in/security-researchers-need-legislative-protection-from-vexatious-lawsuits/ (IFF 2020)
16. Internet Freedom Foundation (2021a). Clause 7 of CERT-In's Responsible Vulnerability Disclosure and Coordination Policy, 3 September 2021. https://internetfreedom.in/dont-penalise-cybersecurity-researchers/ (IFF 2021a)
17. Internet Freedom Foundation (2021b). MeitY. https://internetfreedom.in/over-to-you-meity/ (IFF 2021b)
18. Wilson Sonsini Goodrich & Rosati (2022). https://www.wsgrdataadvisor.com/2022/05/doj-acknowledges-limits-to-the-cfaa-

ISSN: 2582-6433

but-questions-and-possible-civil-liability-remain-for-security-researchers-and-others/ (WSGR 2022)

19. Hogan Lovells (2026). EU Cyber Resilience Act: Preparing for vulnerability and incident reporting. https://www.hoganlovells.com/en/publications/eu-cyber-resilience-act-preparing-for-vulnerability-and-incident-reporting (Hogan Lovells 2026)
20. *India's Cybersecurity Policy Frameworks: Key Strategies and Initiatives | RSM India*. 10 Jan. 2025, https://www.rsm.global/india/insights/consulting-insights/cybersecurity-policy-frameworks.