John Doe Orders – An evolving strategy to mitigate data leaks and cyber-attacks

7 March 2025

John Doe Orders – An evolving strategy to mitigate data leaks and cyber-attacks

Executive Summary

1. Cyber-attacks have become a significant risk for corporate India, often leading to large and high-profile data leaks, that include sensitive personal data belonging to thousands if not lakhs of the company's customers.
2. Injunctions granted against unidentifiable third parties, a creation of India's intellectual property laws, have evolved into a remedy available to a company whose data has been compromised.
3. The evolution of this remedy presents a new mitigation strategy for companies seeking to limit the damage / liability that could arise from a large data leak or cyber-attack that compromises personal data which it holds as a data fiduciary.

Introduction

4. India's large insurance providers have been subject to relentless cyber-attacks since 2024. Several large insurance providers have confirmed that their sensitive customer data has been breached by these attacks[1].
5. India's largest private health insurer, Star Health and Allied Insurance Co. Ltd.("**Star**") is still dealing with the ramifications of a cyberattack that saw 3.1 crore customers' data being leaked online, apparently by an unidentified hacker. It is learnt that the hacker demanded a ransom from the company, while hosting a website and telegram channels that shared samples of the data to users. The leaked data included claim documents and tax details[2].
6. The most recent cyberattack in the sector came in February 2025, when Niva Bupa Health Insurance Co. Ltd. ("**Niva Bupa**") reported that it was investigating leakage of customer data when it received an anonymous ransom demand from a person claiming to be a hacker who had access to the company's data[3].

---

[1] Times of India Tech Desk, '*HDFC Life faces data breach; read company's BSE filing informing customer data hacking*', Times of India, 26 November 2024.
[2] Munsif Vengattil and Aditya Kalra, '*India's Star Health says it received $ 68,000 ransom demand after data leak*', Reuters, 12 October 2024.
[3] Aleef Jahan and Savio D'Souza, '*India's Niva Bupa Health Insurance says it is probing claims of data leak*' Reuters, 21 February 2025.

7. Both Star and Niva Bupa, being headquartered in the presidency towns of Chennai and New Delhi respectively, approached the High Courts of Madras and Delhi seeking *ex parte* injunctions against the dissemination of their data.
8. The decisions of the Madras High Court and Delhi High Court are not binding precedent, since they are interim orders and not judgements that finally adjudicate the matter.
9. Despite this, these orders offer an interesting perspective on the evolution of the remedy of a John Doe Order, usually resorted to in intellectual property disputes, and its blending with a direction that could be regarded as a 'takedown order' under the Information Technology Act, 2000 ("**IT Act**").

John Doe Orders as interim relief

10. Indian Courts have granted 'John Doe' or 'Ashok Kumar' orders for nearly two decades now in intellectual property disputes. The first such order in a civil matter appears to be a decision of the Delhi High Court in *Taj Television Ltd. v. Rajan Mandal and Others*[4].
11. In a dispute involving the unauthorised mirroring of the popular 'Ten Sports' television channel by cable TV operators, many of whom were unknown, the Delhi High Court granted an interim relief in the nature of a John Doe order.
12. It appointed a Court Commissioner to undertake searches of cable operators to collect evidence on whether the plaintiff's channel was being telecast without authorization. Based on the Court Commissioner's report after these searches, the Court would consider issuing notice to these cable operators to arraign them in the proceeding before it.
13. The Courts have also recognised the limits of John Doe Orders in the digital age when dealing with applications requesting takedown orders in respect of entire websites. Whether a takedown order must be in respect only to offending content or to websites hosting such content has been an ongoing debate.
14. The Bombay High Court in *Balaji Motion Pictures and Anr v. BSNL and Ors*.[5], discussed the criticism levelled at John Doe Orders in the digital era, against websites, being too

[4] *Taj Television Ltd. v. Rajan Mandal and Ors.* | [2003] FSR 22
[5] *Balaji Motion Pictures and Anr v. BSNL and Ors* | Order dated 4 July 2016 in Notice of Motion (L) No. 1940 of 2016 in Suit (L) No. 694 of 2016.

broad and resulting in the entire website including legitimate content being blocked or taken down.

15. When it was approached for an ad interim injunction against the online piracy of a Bollywood movie, the Court refused to grant the injunction when the application seeking it was framed to seek a John Doe Order in respect of websites.
16. It was only when the application was reframed to identify individual URLs containing the offending content, that the Court granted the relief of ordering the blocking of access to the links, allowing the plaintiff to seek the blocking of further URLs they found subject to an assessment by the Cyber Crime Cell and injuncted intermediaries and television service providers from unauthorised broadcasting of the movie.
17. Interestingly the Court directed the publication of its order and observed that this would constitute sufficient service on the John Doe defendants.
18. In the context of a data leak / cyberattack where large amounts of sensitive personal data, often belonging to thousands if not lakhs of citizens, it remains to be seen whether Courts will observe that there exists a public interest element that must be balanced with a website / platform's right not be blocked entirely due to this data being hosted on it.

Safe Harbour for Internet Intermediaries

19. The IT Act, under Section 79, provides exemptions to intermediaries from liability over data hosted on their platforms upon the fulfilment of certain conditions. The provision applies to intermediaries whose role doesn't involve initiating a transmission of information, selecting the recipient or modifying the information hosted on its platform.
20. The 'safe harbour' under Section 79 can be lost if an intermediary, upon receiving 'actual knowledge' from the appropriate Government or its agencies, fails to remove or block access to information / computer systems on its network that are being used to commit an unlawful act[6].
21. The Supreme Court of India, in its landmark ruling in *Shreya Singhal v. Union of India*, a decision that arose from a Public Interest Litigation filed by a student, struck down Section 66A of the IT Act, an often misused provision that punished 'offensive messages' transmitted online.

[6] Section 79(b) of the Information Technology Act, 2000.

22. In its decision the Supreme Court also read down Section 79(3)(b) of the IT Act, to mean "*that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material*"[7], in which circumstance, the safe harbour the intermediary enjoyed under Section 79(1) would not apply.
23. This reading down of the term *'actual knowledge'*, limited it to mean only orders of a Court of competent jurisdiction.
24. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 ("IT Rules 2021") have, however, increased the scope of '*actual knowledge*', to mean – "*actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency...*" [Emphasis Supplied].
25. It is the author's view that the above Rule is *ultra vires* Section 79 (3)(b) of the IT Act, which has been read down by the Supreme Court of India. While it remains to be seen whether the *vires* of the provision will be challenged, presently there appears to be some ambiguity in what the phrase 'appropriate government or its agencies' means.
26. The Ministry of Electronics and Information Technology has notified a list of nodal officers of the Central Government who may issue notices under the IT Rules 2021[8]. The prevailing view seems to be that these officers are the authorities empowered to issue takedown orders.

The Commercial Suits

Star Health Dispute

27. The insurance companies, Star and Niva Bupa, approached the Madras High Court and the Delhi High Court respectively, and sought *ex parte ad interim* orders against several parties including Domain Name Service Providers, Internet Service Providers and the Central Government to prevent or 'take down' their data which had been illegally obtained.

---

[7] *Shreya Singhal v. Union of India* at [117] | 2015 5 SCC 1

[8] List of Nodal Officers from Ministries / Departments of Central Government under the provisions of Information Technology (Procedure and safeguards for blocking access of information by public) Rules 2009 - https://www.meity.gov.in/static/uploads/2024/12/b7a2d484bf95cd842ddd505f6fdd23b2.pdf

28. Star approached the Madras High Court in a Commercial Suit before the High Court's Commercial Division on 24 September 2024, arraying Telegram FZ LLC, Cloudflare India Pvt. Ltd., Cloudflare Inc, Ashok Kumar[9] and 'Xenzen'.
29. 'Xenzen' is the name the hacker allegedly used in his communications with Star, while Cloudflare is a popular Domain Name System Provider, and Telegram FZ LLC ("**Telegram**") is a Dubai based company that operates the 'Telegram' messaging platform known for its focus on anonymity.
30. Star sought an *ex parte ad interim* injunction against the defendants from disseminating its data on the Telegram platform and over websites. While this order is not accessible through the Madras High Court's website, it has been reported that the Madras High Court, on 24 September 2024, granted the *ex parte ad interim* injunction and directed Telegram to block Xenzen and any chatbots being used to make Star's data available on the platform. It is understood that a similar direction was issued to the Cloudflare entities to ensure that websites hosting Star's data were taken down or blocked.
31. Telegram appeared before the Madras High Court and submitted that it could and would comply with any order where it was directed to take down accounts that Star identified as being ones that shared its data. It submitted that it could not patrol the platform to find accounts that were disseminating Star's data[10].
32. Telegram's submissions seem to be based on the settled proposition of law that takedown notices issued under the Information Technology Act, 2000 to an intermediary such as Telegram, must be specific and the information whose access is sought to be restricted must be identifiable.
33. The Madras High Court through an order dated 25 October 2025, modified its earlier directions to state that Telegram would only be required to remove or block access to chatbots and channels that Star specifically identified as sharing its data. Notably this direction came to be passed after Telegram volunteered to take down accounts flagged by Star.

---

[9] An Unidentified Male is referred to in Western Jurisdictions as "John Doe", while an unidentified female as "Jane Doe". India has an equivalent for an unidentified male – "Ashok Kumar". Orders against unidentified third parties are interchangeable referred to as Ashok Kumar Orders or John Doe Orders.

[10] Upasana Sanjeev, '*Star Health Data Breach: Telegram agrees to take down accounts flagged by Star posting user information, says can't do patrolling'*, Livelaw, 25 October 2024.

Niva Bupa Dispute

34. The Delhi High Court, approached by Niva Bupa this year, took a slightly different approach to the issue. The company approached the Delhi High Court in a Commercial Suit[11] against several Domain Registration Providers, Internet Service Providers, the Department of Telecommunications and Information Technology and an unidentified defendant.

35. Niva Bupa sought comprehensive directions by way of interim relief in addition to an *ex parte ad interim* injunction against 'Xenzen', the hacker, to not disseminate the confidential data leaked from Niva Bupa.

36. The Delhi High Court examined the emails received from Xenzen, arrayed as Defendant No. 15 in the suit, and found that there was a *prima facie* case made out for the theft of confidential data belonging to Niva Bupa.

37. The Delhi High Court also noted that the Defendant No. 15 claimed to be the hacker responsible for the Star data leak and a connected pending matter filed by Nuva Bupa seeking orders similar to the ones passed by Madras High Court in the Star case, against Telegram. Based on this, the Delhi High Court noted that there was an eminent danger that Niva Bupa's confidential data might be leaked online.

38. The Court observed that the action before it was a *quia timet* (latin for – 'arising from apprehension') action.

39. The Delhi High Court issued the following order:

    (a) Defendant Nos. 1 – 14 were directed to take down, remove/permanently block two specific websites identified as hosting Niva Bupa's confidential data;

    (b) Defendant Nos. 1 – 14 were directed to take down, remove / disable email addresses through which Defendant No. 15 has been communicating with Niva Bupa;

    (c) Defendant No. 15 and its connected persons and entities were restrained from inter alia publishing Niva Bupa's data on any medium or platform whatsoever;

    (d) Defendant No. 15 and its connected persons and entities were restrained from infringing on Niva Bupa's trademarks including the use of 'Bupa' in any form of

---

[11] *Niva Bupa Health Insurance Company Ltd. v. Nicenic International Group Company Ltd. and Ors.* | CS (COMM) 171/2025

media and inter alia as part of domain IDs, email IDs and in any manner on the internet;

(e) The Defendant Nos. 1 – 13 were directed to provide information on the users who registered the websites / email addresses through which the confidential data was disseminated.

(f) Defendant Nos. 13 and 14 (presumably the Ministry / Department of Electronics and Information Technology) were directed to instruct registered internet service providers, intermediaries and other organizations to disable, block and remove the websites and email addresses identified in the suit.

(g) Further websites, domain names, content and accounts along with associated email addresses and phone numbers that are used to disseminate, leak or publish Niva Bupa's confidential data, which are identified by the Plaintiff on an affidavit before the Joint Registrar (Judicial) of the Delhi High Court. The directions of the Court would be applicable to these subsequent websites, accounts, content and domain names identified in the affidavit.

40. The Delhi High Court's order grants *ex parte ad interim* reliefs that are usually seen in intellectual property matters where copyright information is being illegally utilized or trademarks are being passed off.

Conclusion

41. What follows from the recent decisions of Indian Courts where the interim relief of John Doe orders are granted ordering the takedown of content from a website, intermediary or online platform, is that a new remedy has evolved over time and through the ingenuity of India's Courts and the bar.

42. This remedy, finding its roots in intellectual property disputes, has emerged as an effective way for a company dealing with a cyberattack or a large scale data breach. The orders of the Madras High Court and the Delhi High Court passed in the context of the recent cyberattacks on private insurance companies, indicate that this remedy will receive increased examination and refinement in the years to come.

43. The introduction of the Digital Personal Data Protection Act, 2023 has created a statutory requirement for data fiduciaries to inform data principals of data breaches. There are also regulatory requirements that are laid down in certain sectors that deal with large amounts of personal data.

44. The Reserve Bank of India has prescribed the Cyber Security Framework for banks, while the Insurance Regulatory and Development Authority of India has prescribed Cyber Security Guidelines for insurers.

45. Apart from these regulatory requirements, companies can also face civil claims and consumer disputes where it can be proved that they did not exercise due diligence or follow either prescribed or prevailing industry standards on cyber security leading to sensitive personal data being leaked.

46. In this backdrop, a John Doe order framed for the removal of this sensitive data becomes the cornerstone of a liability or damage mitigation strategy that an affected company must take when faced with a large data leak or cyber-attack.