

Delhi High Court Refines the Dynamic Injunction Framework for Rogue Websites

Home Box Office Inc. & Ors. v. Streamzy.to & Ors.

CS(COMM) 740/2026 | I.A. 18203/2026 | Neutral Citation: 2026:DHC:5967

High Court of Delhi at New Delhi

Coram: Hon'ble Mr. Justice Anup Jairam Bhambhani | Date of Order: 27 July 2026

In Brief

- The Delhi High Court has granted an ad-interim injunction restraining thirty identified rogue streaming websites, together with directions to the concerned internet service providers to block access and to the Department of Telecommunications and the Ministry of Electronics and Information Technology to notify the wider body of registered ISPs.
- The order's more lasting contribution lies elsewhere - in how the Court has further calibrated the "dynamic injunction" mechanism used to prevent rogue websites from resurfacing under mirror or redirect domains once blocked.
- The Court draws a considered distinction between conferring adjudicatory discretion on internet service providers and domain name registrars, which it holds impermissible, and asking them to perform a narrow, technical verification exercise, which it holds does not compromise their neutrality under Section 79 of the Information Technology Act, 2000.

Background

The suit was instituted by Home Box Office Inc., together with other producers and rights-holders, against thirty websites, led by Streamzy.to, accused of streaming the plaintiffs' copyrighted cinematographic works without licence. The remaining defendants comprise the domain name registrars who registered these websites (Defendant Nos. 31 to 50), the internet service providers through whom Indian subscribers access the internet (Defendant Nos. 51 to 59), and the Department of Telecommunications and the Ministry of Electronics and Information Technology (Defendant Nos. 60 and 61), being the authorities empowered to direct the wider ISP community to block access. By way of I.A. 18203/2026, filed under Order XXXIX Rules 1 and 2 read with Section 151 of the Code of Civil Procedure, 1908, the plaintiffs sought an ad-interim injunction against the websites, coupled with corresponding blocking and notification directions.

Identifying a Rogue Website: The FIOL Test

The Court's starting point was the now well-settled test for identifying a "Flagrantly Infringing Online Location" or FIOL, laid down by a coordinate bench of this Court in *UTV Software Communication Ltd. v. 1337X.To*, 2019 SCC OnLine Del 8002. That decision rejected the proposition that infringement on the internet warrants more indulgent

treatment than infringement in the physical world, and set out a non-exhaustive list of factors bearing on whether a website is a rogue website - among them, whether its primary purpose is to commit or facilitate infringement; the flagrancy of that infringement; whether the registrant's details are masked and untraceable; whether the site has ignored takedown notices; whether it hosts indexes or directories of infringing material; whether courts elsewhere have already disabled access to it; and the volume of traffic it draws.

Applying this test, the Court found, on a prima facie basis, that Defendant Nos. 1 to 30 bore the hallmarks of FIOs: their registrant details were masked, no traceable contact information was available, and the content made accessible on the sites was, on the material before the Court, overwhelmingly unlicensed cinematographic content belonging to the plaintiffs. This was, in the Court's assessment, not a case of incidental infringement, but one in which facilitating infringement was the primary purpose of the websites (para 7).

The Central Difficulty: A Moving Target

The more substantial question before the Court concerned enforcement once an injunction is granted. Rogue websites routinely respond to a blocking order by re-emerging under mirror, redirect, or alphanumeric variant domains, leaving the rights-holder to chase what the Court itself described as a moving target (paras 14-15). Notably, the risk of an unqualified solution to this problem was flagged not by the enjoined websites but by two of the domain name registrars named as defendants, who, while raising no objection to blocking the websites actually identified in the suit, pointed out that an open-ended direction to block any future website merely on the plaintiffs' say-so would require them, as neutral intermediaries, to exercise a blocking power without any administrative or judicial order behind it (para 13).

This Court and its coordinate benches have, over a series of orders, developed varying answers to this problem, generally described as "dynamic" or "Dynamic+" injunctions, permitting a rights-holder to bring newly discovered mirror websites within the scope of an existing order without instituting fresh proceedings for each one. The present order surveys five such precedents (paras 16.1 to 16.5), ranging from mechanisms routed through a formal impleadment application before the Joint Registrar, to mechanisms permitting internet service providers and domain registrars to act directly on a rights-holder's intimation, subject to a subsequent affidavit before the court and a reserved liberty for the intermediary to object.

The Court was unwilling to adopt either extreme. Requiring the plaintiffs to return to court each time a mirror site surfaces would make the injunction largely illusory (para 15). But allowing the plaintiffs, the internet service providers, or the domain registrars an unsupervised carte blanche to block any website they consider a mirror site would hand a private party the adjudicatory function of deciding what is "rogue" - a function the Court held an ISP or DNR, as a neutral intermediary, is neither equipped nor authorised to discharge, and one the plaintiffs cannot assume for themselves under the guise of a blocking direction (paras 19-20).

The Court's Solution: Technical Verification, Not Adjudicatory Discretion

The order's central contribution is the distinction it draws between two functions that can look similar on the surface but are, in the Court's view, of a different order altogether: first, the discretion to decide whether a website is

infringing and ought to be blocked, which must remain exclusively judicial; and second, the narrower, ministerial task of verifying whether a website the rights-holder identifies as a mirror site is, in fact, a mirror, redirect, or alphanumeric variant of a website already found, at least prima facie, to be infringing, which may permissibly be delegated to the internet service provider or domain registrar concerned (para 22).

On this footing, the Court directed a mechanism with four working parts, to operate pending the next hearing (paras 21.1 to 21.4):

- the ad-interim injunction against Defendant Nos. 1 to 30, the corresponding blocking direction to the internet service providers, and the notification direction to the Department of Telecommunications and the Ministry take immediate effect;
- where the plaintiffs discover a mirror, alphanumeric, or redirect website, they may furnish an affidavit with supporting documentation to the concerned internet service provider or domain registrar, who must then technically verify whether the site is in fact a mirror of an already-injuncted website and, if satisfied, enforce the injunction against it as a pro-tem measure;
- simultaneously with that affidavit, the plaintiffs must also move an application before this Court under Order I Rule 10 of the Code of Civil Procedure seeking impleadment of the newly discovered website, so that the mechanism does not operate wholly outside the suit; and
- any assertion by the plaintiffs, whether before the intermediary or before the Court, that is later found to be baseless, false, or not bona fide, will invite appropriate orders from the Court.

The Court has also preserved a corresponding safeguard for the intermediaries: an internet service provider or domain registrar retains the liberty to approach the Court to resist a blocking request, and any blocking undertaken under this mechanism remains, without exception, a pro-tem measure liable to variation on further directions (paras 23-24). In this respect, the order is more exacting than some of the precedents it surveys - for instance, under the order in *Home Box Office Inc. v. Moviebox.ph & Ors.* (order dated 06.04.2026 in CS(COMM) 358/2026), the plaintiff's recourse to the Joint Registrar for impleadment was left to its liberty; here, filing such an application is made a mandatory, simultaneous part of the same mechanism, and the intermediary's role is expressly confined to technical verification rather than a blocking discretion at large.

The Court reconciles this with the settled position on intermediary liability by holding that what is delegated to the internet service provider or domain registrar is not the discretion to block that Section 79 of the Information Technology Act, 2000, read with the Supreme Court's judgment in *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, at paragraphs 121-122, denies to a neutral intermediary, but only a factual, technical question: whether a given URL is a mirror of a website already found to be infringing. Because the substantive determination of infringement continues to rest with the judiciary, the Court did not consider this arrangement to place the intermediaries' safe-harbour protection at risk (para 22).

Practical Implications

For rights-holders - producers, broadcasters, and OTT platforms:

- A dynamic injunction remains available to bring newly discovered mirror or redirect websites within an existing blocking order without a fresh suit, but relief of this kind will likely now require both an affidavit-backed intimation to the ISP or DNR and a simultaneous impleadment application before the court - an intimation to the intermediary alone is unlikely to suffice going forward, at least before this Bench.
- Because a false or careless assertion that a site is a "mirror" can invite adverse orders, rights-holders should maintain a defensible internal record of how each new website was verified before triggering enforcement.

For internet service providers and domain name registrars:

- Your role under this mechanism is limited to technical verification, not a substantive finding of infringement, a distinction the Court has taken some care to preserve, and one that should ease safe-harbour concerns around participation in such mechanisms.
- The liberty to approach the Court to resist a blocking request you consider unwarranted remains expressly available to you, and any blocking you undertake is only ever a provisional, pro-tem measure.

A Note on Procedural Posture

This is an ad-interim order passed at the notice stage. The defendants who have entered appearance have thirty days to file their replies, with a further thirty days for any rejoinder, and the prima facie findings recorded here, including the finding that Defendant Nos. 1 to 30 are FIOs, remain open to being tested at final adjudication.

Disclaimer: *This update has been prepared for general informational purposes only and does not constitute legal advice. We would be pleased to discuss the implications of this judgment as they may pertain to any specific matter.*