Q300-RES-G-2026

2026 AIPPI World Congress – Hamburg
Adopted Resolution
10 October 2026

Resolution

2026 – Study Question – General

Dynamic Blocking Injunctions

Background:

1) This Resolution concerns the recognition of Dynamic Blocking Injunctions as a remedy to tackle online intellectual property (IP) infringement, their scope and availability, the principles governing their grant, implementation, duration and review, and the need to balance effective IP enforcement with other legitimate rights and interests.

2) For the purposes of this Resolution, "Dynamic Blocking Injunction" (DBI) refers to an injunctive order designed to address online IP infringement by enabling it to extend, without the need to commence fresh proceedings, to subsequently identified online locations, access points or content falling within the scope of the original order.

3) The digital age has led to a proliferation of large-scale online IP infringement in the form of, for example, "hydra-headed" mirror websites, proxies, live-stream piracy, cyber-lockers and other online locations that can rapidly clone, redirect or relocate their operations. There is a broad consensus that conventional or "static" injunctions - which are limited to a set of identified defendants or online locations and require right holders to repeatedly approach courts for new orders - may be insufficient to effectively address rapidly evolving and adaptive forms of online IP infringement.

4) Over the past decade, DBI has been recognised or granted in a number of jurisdictions, particularly in the context of copyright piracy and unauthorised live

streaming, and increasingly in relation to other forms of online IP infringement. Depending on the applicable legal framework, such injunctions may be directed against infringers, against intermediaries whose services are used in connection with the infringement without requiring any finding of liability on their part for the underlying infringement, or against both. International and regional initiatives have also highlighted their potential role as an effective enforcement mechanism, subject to appropriate safeguards against disproportionate over-blocking and interference with legitimate interests.

5) Cross-jurisdictional (i) recognition (ii) implementation and (iii) enforcement of DBI is not addressed by this Resolution. Issues concerning costs and damages are also outside the scope of this Resolution.

6) 36 Reports were received from AIPPI's National and Regional Groups and Independent Members providing detailed information and analysis regarding national and regional laws relating to this Resolution. These Reports were reviewed by the Reporter General Team of AIPPI and distilled into a Summary Report (which can be found at www.aippi.org).

7) At the AIPPI World Congress in Hamburg in 2026, the subject matter of this Resolution was further discussed within a dedicated Study Committee, and again in a full Plenary Session, following which the present Resolution was adopted by the Executive Committee of AIPPI.

AIPPI Resolves that:

Recognition

1) It is desirable to have global recognition of DBI to ensure effective enforcement against certain online IP infringement.

2) National and regional legal frameworks should provide clear rules and/or principles governing DBI, including their grant or refusal, modification or revocation, appeal, implementation, including a requirement for expeditious procedures, as well as appropriate safeguards to ensure a proper balance between IP rights, freedom of expression and other public interest considerations.

Scope and Applicability

3) DBI should be available to enforce at least:

- Copyright and neighbouring/related rights;
- Trademarks;
- Designs;
- Geographical indications.

Typical examples of infringing conduct for which DBI could be granted include audiovisual, music and literary piracy, unauthorised live streaming of time-sensitive events, online counterfeiting, illegal online marketplaces, AI-generated content and deepfakes.

4) National and regional legal frameworks may decide whether DBI should be available in cases involving patent infringement, taking into account the complex technical or legal assessments that may be required in such cases and/or may make DBI inappropriate in certain circumstances.

5) National and regional legal frameworks may decide whether DBI should be available in cases involving the unlawful acquisition, use or disclosure of trade secrets, taking into account the issues of confidentiality and complex legal assessments that may be required in such cases and/or may make DBI inappropriate in certain circumstances.

6) While issuing DBI, care should be exercised to avoid the disproportionate over-blocking of lawful content or activities, unintended chilling effects and/or disproportionate interference with (i) legitimate business activities, (ii) freedom of expression or (iii) access to information.

Practice and Procedure

7) The authority to grant DBI should reside with courts and/or other appropriate institutions competent to issue injunctions. The implementation thereof can be delegated to other authorities, as permissible under national or regional legal frameworks.

8) National and regional legal frameworks may determine the factors to be taken into account when deciding whether to grant or refuse a DBI. Such factors may include, where relevant:

- Proof of a clear *prima facie* case of IP infringement;
- The nature, extent and urgency of the actual or potential harm;
- The proportionality and necessity for the grant of the DBI;
- The flagrancy of infringing conduct;
- Whether the primary purpose of the relevant website or online service is to facilitate or commit IP infringement;
- The operator's deliberate falsification or concealment of its true identity, or use of anonymity;
- Silence, refusal to comply or inaction following receipt of formal legal notices;
- Reappearance or mirror-cloning across alternative domains or IP addresses following prior enforcement actions; or
- Compliance with any applicable requirements of due process.

9) The scope of a DBI should be proportionate to the nature and extent of the infringing activity. Blocking measures should be appropriately targeted and/or applied to avoid disproportionate interference with lawful content, freedom of expression or legitimate commercial activities.

10) A DBI may be directed against any relevant intermediary, including Internet Service Providers (ISPs), alternative DNS providers, Domain Name Registrars (DNRs), content delivery networks (CDNs), Hosting Service Providers (HSPs), e-commerce platforms, app aggregators, social media networks and payment intermediaries, and where necessary and proportionate for its effective implementation. The grant of a DBI should not, in itself, imply liability on the part of the intermediary for the underlying infringement.

11) DBI should remain in force only for so long as is necessary and proportionate in the circumstances and should be subject to review mechanisms.

Review, Modification and Revocation of DBI

12) The grant or refusal of a DBI should be subject to a right of review or appeal, which will not necessarily have suspensive effect. Any person materially affected by a DBI should have an effective means of seeking the modification, revocation or termination of the DBI where appropriate.

13) National and regional legal frameworks may determine the grounds on which a DBI may be modified, revoked or terminated, upon request of the plaintiff, an infringer, an affected intermediary, or any other person materially affected by a DBI. Such grounds may include, where relevant:

- The DBI is no longer necessary, or circumstances justifying it have ceased to exist without a significant risk of recurrence;
- Circumstances justifying an amendment to the scope of the DBI;
- Material misrepresentation, concealment, or bad faith by the plaintiff;
- Abuse of the DBI resulting in restriction of lawful competition or non-infringing services;
- Failure to comply with the terms of the DBI, including implementation/reporting requirements, if any;
- Unintended chilling effects, disproportionate over-blocking of lawful content, disproportionate interference with (i) legitimate business activities, (ii) freedom of expression or (iii) access to information.