



Christian Dawson
Executive Director
Internet Infrastructure Coalition (i2Coalition)

March 17, 2026

Kurtis Lindqvist
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

Dear Kurtis,

The Internet Infrastructure Coalition (i2Coalition) writes to bring to your attention a recent judicial development in India that raises important considerations for the Internet governance ecosystem and the role of the multistakeholder model in defining the responsibilities of DNS operators. Developments of this kind may also have implications for the Internet community's longstanding goal of maintaining "One World. One Internet."

On December 24, 2025, the Delhi High Court issued a ruling in *Dabur India Limited v. Ashok Kumar and Ors.*, a trademark-related case that significantly expands the legal and operational obligations placed on domain name registrars and registries. While the case arises from a domestic intellectual property dispute, several elements of the ruling appear to impose obligations on DNS infrastructure operators. These obligations extend beyond the roles currently defined through ICANN's multistakeholder policy processes and contractual framework.

Among other provisions, the ruling appears to:

- Require registrars to disclose registrant data within 72 hours upon request;
- Mandate permanent blocking of domains deemed infringing, along with similar or variant domains not proven to be infringing;
- Require proactive denial of future domain registrations incorporating certain "well-known" trademarks absent a judicial finding of infringement;
- Mandate the collection of registrant identity data in a prescribed national format; and
- Impose liability on registrars and registries for alleged trademark violations by registrants.



Certain obligations described in the ruling may also be technically infeasible for some DNS operators to implement within existing provisioning systems. For example, requirements to proactively deny future registrations incorporating certain trademarks could require registries to make adjudicative determinations or conduct screening functions that are not currently supported by DNS provisioning models.

More broadly, the decision raises questions about the appropriate boundaries between national judicial enforcement and the globally coordinated governance framework for the Domain Name System. Registrars and registries operate within a carefully structured contractual and policy environment developed through ICANN's multistakeholder processes. Through those processes, the ICANN community has historically defined the limited and clearly scoped responsibilities of DNS operators in order to preserve the stability, interoperability, and security of the global Internet. When obligations affecting those roles emerge outside that framework, it can create uncertainty for operators subject to ICANN contractual requirements while simultaneously facing national legal mandates that may not align with established technical coordination processes.

When courts impose obligations that redefine those responsibilities outside this framework, it risks creating inconsistent expectations across jurisdictions and increasing operational uncertainty for globally operating infrastructure providers. If replicated across jurisdictions, rulings of this nature could create conflicting legal obligations for DNS operators operating under globally coordinated technical standards.

Infrastructure-layer enforcement mechanisms such as DNS blocking also carry inherent risks of overbroad impact. Because DNS operators generally cannot remove specific content hosted on websites, their primary technical mechanism is domain suspension or blocking. Such actions can result in full service disruption affecting lawful content and unrelated activities associated with a domain name. Mandating enforcement at the DNS layer, therefore, risks collateral disruption that extends beyond the alleged infringement at issue.

The ruling may also introduce privacy and cybersecurity considerations. Requirements to collect registrant identity data in prescribed national formats, combined with rapid disclosure obligations and changes to privacy protections, could create tensions with globally harmonized domain registration data practices while increasing the concentration of sensitive personal data within infrastructure systems.

Taken together, developments of this kind may signal a broader pattern in which courts seek to address intellectual property or content disputes by imposing obligations at the infrastructure layer rather than at the hosting, platform, or content layers. If such approaches become more widespread, they could place increasing pressure on the DNS ecosystem and create fragmentation risks inconsistent with the goal of maintaining a single, globally interoperable Internet.



We recognize that ICANN does not intervene in national judicial proceedings. However, developments of this nature raise questions that touch directly on ICANN's mission to support the stable and secure operation of the DNS and the multistakeholder processes through which DNS operator responsibilities are defined.

For that reason, we believe it would be valuable for ICANN org and the broader community to remain aware of this development and to consider whether additional dialogue within the multistakeholder framework may be warranted regarding the appropriate scope of infrastructure-layer obligations.

We appreciated the opportunity to discuss related issues with members of the ICANN community during ICANN85 in Mumbai and would welcome the opportunity to provide further technical context to ICANN org or relevant community groups if helpful.

Thank you for your continued leadership in supporting the stability and global interoperability of the Internet.

Respectfully,

A handwritten signature in black ink, appearing to read 'Christian Dawson', followed by a horizontal wavy line.

Christian Dawson
Executive Director
Internet Infrastructure Coalition (i2Coalition)