Growing accountability of domain name registrars

IMAGE: SHUTTERSTOCK / NIPOWORLD

The courts have given some indication of how much responsibility lies with registrars for domain name abuse, but more effective solutions are needed in this ever-evolving world, says Ashwin Julka of Remfry & Sagar.

In 2022, the Indian e-commerce market was valued at $75 billion, with the potential to grow to $200 billion by 2026. Also, registrations for the top country-level domain '.in' reportedly surpassed 2.5 million in 2021.

But an emergent online marketplace has also led to a proliferation of domain name abuse. Typically, the WIPO's UDRP or its Indian counterpart, INDRP, have helped adjudicate complaints seeking cancellation or transfer of disputed domains.

However, a surge in *malafide* registrants providing fictitious/non-traceable details at the time of registration and operating through channels designed to keep internet activity anonymous, is making it increasingly difficult to identify miscreants and halt misuse.

Shifting the focus from registrant to registrar

The Delhi High Court has been considering this issue of masked identities in a series of suits filed before it (*Dabur India v Ashok Kumar and Ors.*, 2022). The issues for examination include:

- methods available to domain name registrars to verify identities of registrants during registration;
- examining privacy protect features and proxy server options made available to registrants (that can blur their true identity) by registrars—whether on specific request by the former or as a standard feature of a 'bundle';
- methods enabling a registrar to share registrant data with an owner of a well-known brand without court or government intervention;
- appointment of grievance officers by registrars and mechanisms for implementation of court orders (eg for information disclosure).

On all these matters, inputs have been sought from the Department of Telecommunication, Ministry of Electronics and Information Technology (MEITY) and the domain registrar community, and the court will next hear the matter in May 2023. Meanwhile, as of March 27 this year, MEITY had submitted its report stating that 'repeated' non-compliance of court orders by a domain name registrar could result in its website/URL being blocked under Section 69A of the Indian Information Technology Act, 2000 ('IT Act'). Also, lack of due diligence could mean loss of safe harbour protection under the IT Act. In a related development, the Digital India Act—expected to replace the IT Act—is soon to be a reality wherein compliance requirements for intermediaries are set to increase.

The Bombay High Court dealt with domain name abuse in multiple rounds of litigation involving online food delivery service Swiggy. In round one, the court directed suspension of the infringing domain names and asked GoDaddy to not register any domain name containing Swiggy's trademarks without prior authorisation. GoDaddy appealed, arguing that the domain name registration process was automated and ruled out prior authorisation. However, Swiggy cited GoDaddy's submission before the Delhi High Court in a different suit (*Snapdeal Pvt v GoDaddy.com*): "subject to technical, financial and resourcing issues, the said defendant could potentially prevent a user from registering names with the exact word, in respect of which the plaintiff holds a registered trademark."

Watering down the ruling in round two, the court directed GoDaddy to inform Swiggy whenever a domain name containing the trademark 'Swiggy' was registered. GoDaddy appealed again, contending that domain names could be registered with any one of 2,600 registrars globally and imposing an onerous responsibility on GoDaddy alone was overreaching. This time the court agreed with GoDaddy. It held that registrars can only suspend the registration of specific domain names found to be infringing and cannot be expected to permanently block registration without a finding of fraudulent behaviour.

"Interestingly, countries including the UK have laid down strict conditions for availing domain privacy and proxy services offered by registrars."

Looking ahead

Courts in India seem to be tightening their grip on domain name registrars to address misuse, but at the same time are being mindful of stakeholders' rights. Interestingly, countries including the UK have laid down strict conditions for availing domain privacy and proxy services offered by registrars. For instance, only non-trading domain name holders (not a business or organisation) can opt out of having address details published on the WHOIS database. Though this has spawned a debate on privacy, what seems to emerge is a growing attempt across jurisdictions to increase accountability of domain name registrars.

Developments such as blockchain domain names that operate outside ICANN's domain name systems pose fresh challenges. Blockchain transactions are carried out through a pseudonym, making potential recourse even more difficult than it is for traditional domains. The need to look for more effective solutions has, therefore, never been more urgent. ●

Ashwin Julka is managing partner of Remfry & Sagar. He can be contacted at: ashwin.julka@remfry.com