Journal of Intellectual Property Rights
Vol 30, November 2025, pp. 754-762
DOI: 10.56042/jipr.v30i6.14563

Navigating the Masking Dilemma: Addressing the Controversy Surrounding Masked Registrant Information by Domain Name Registrars (DNRs)

Atal Mishra[1†], Saket Sharma[2] and Neha Tripathi[3]

[1] National Law University, Jodhpur – 342 304, India

[2]Galgotias University, School of Law, Greater Noida – 203 201, India

[3]Mahindra University, School of Law, Bahadurpally Jeedimetla, Hyderabad – 500 043, India

Received: 5th November 2024; revised: 28th April 2025

Proliferation of domain names that closely resemble well-known trademarks and brands has led to a significant increase in online consumer fraud in India. These imposter domains have deceived countless individuals, resulting in substantial financial losses. Numerous instances in India demonstrate the widespread impact of this issue, with victims falling prey to phishing scams, counterfeit goods, and other fraudulent activities. Anonymity of domain name registrants has facilitated such fraudulent online activities. Many individuals and organizations have exploited the privacy options offered by domain name registrars (DNRs) to conceal their identities and engage in deceptive practices. This has contributed to the ongoing challenges of combating online fraud and protecting consumers from harm. Ideally, while making huge commercial gains such entities should not be able to escape the liability in the garb of protecting privacy of the offenders. However, DNRs have also taken a stand that they do not have any permanent establishment in India, and they are not bound to follow Indian law as they are not signatory to the Registrar Accreditation Agreements (RAA) which bound them to provide all the relevant information to the concerned authorities in India. This paper analyses the challenges faced by the authorities in providing redressal to the consumer frauds due to opaque disclosure policy of DNRs by encapsulating the struggle between privacy and transparency. This paper examines the legal and enforcement challenges in ascertaining liability of DNRs in cases of consumer deception and fraud by imposter domain names providing services in India. The paper finally provides possible suggestions to shape effective guidelines which shall be useful for policymakers and enforcement agencies.

Keywords: DNRs (Domain Name Registrar), Cyber-Squatting, Transparency, Masking, Privacy

Domain names have evolved as a pivotal medium for enterprises in the digital market to carry out their business. A sudden surge in the growth of online businesses was observed as they were compelled to shift to digital mode as physical markets were completely shut down during Covid. This shift of the economy to the digital mode has given rise to a plethora of issues pertaining to the registration of domain names.[1] The trader is provided a domain name by the Domain Name Registrars "(DNRs)", then a website is created in the name of his business where he promotes the product and services. The vast reach of internet has made the domain names user-friendly as it directs the customers to businesses in just one tap. Unfettered registration of the domain names by DNRs has given rise to alarming issues in India. Considering such situation this paper will address the questions underlying these prominent issues that are pertinent to the optimal regulation of DNRs in India. Such underlying questions are: Whether DNRs can be included within the meaning of "intermediaries" under the Information Technology Act, 2000 (IT Act, 2000)? Does the provision of privacy protection by DNRs render their actions illegal? Whether DNRs are bound to disclosure of identity of the registrant upon the court direction and for investigation purpose? What are the best practices for DNRs to register domain names in India, considering factors like privacy, security, and legal compliance?

This research paper examines the ambiguities pertaining to the registration of Domain Names and critically analyses their privacy protect feature. Now Domain Names have achieved a significance position in the digital market, considering this a contention have been bought forth that DNRs should be considered as the Intermediaries under the information technology act so that they can be held liable for ongoing discrepancies with respect to their stand in the disclosure of the registrant information.

†Corresponding author: Email: atalmishrarbl@gmail.com

This section gives a brief introduction about the importance of DNRs in digital market and addresses the research questions. The second section gives a broad summary of Indian Legal Framework which regulates the Domain Name Registrations. The third section covers the discussion of DNRs as the Intermediaries under the IT Act, 2000. The fourth section examines the issue of masking registrant identity by the DNRs. In the fifth section, an attempt was made to compare the legal systems in India, the United States, and the European Union, along with the role of global organizations in regulating DNR abuse. The sixth section proposes the legal reforms to address and handle the issue adequately. The final portion is devoted to concluding remarks and certain recommendations.

Indian Legal Framework with respect to Domain Name Registration as Trademark

A Domain name is a unique computer address where user is assigned an Internetworking Protocol address (IP Address). It is a combination of certain digits which contains a network portion, and its numeric characters are separated by the periods for the designation of fields that helps the internet users to locate that specific network.[2] Now IP addresses have transformed to the Domain name also known as Uniform Resource Locator "(URL)" to make them user friendly as mnemonic designation has been given to this numeric character.[3] It is difficult for the user to remember long IP addresses in a binary language of the computer, for example www.mnlua.ac.in/library is quite easy to remember rather than 135.181.136.149.[4]

The domain names are combination of three parts where first part is recognized as third level domain which is "www" it represents that the website is connected to the world wide web and it can be discovered by any search engine. The second is the unique name of the company such as 'Amazon'. The last part is known as top level domain name it is of different type such as country code Top-Level Domains "(ccTLD)", generic Top-Level Domains "(gTLD)", international country code top-level domains ('IDN cc TLD') international generic country code Top-Level domains "('IDN gcc TLD)". In top level domain name identifiers used are: ".in" is for the country India or ".au" for Australia etc. "gov", identified as the government networks; ".com", identifies commercial organizations; ".net" is used for the computer site or network organizations; ".edu," is being used by the educational institution; and ".org," is for the identification of non-profit organizations.[5] Domain names have evolved as a digital counterpart of the trademarks and the products and services are being recognized by it in the cyber space. Internet Corporation for Assigned Names and Number "(ICANN)" is the body which regulates the registration of the domain names globally.[6] There are strict guidelines pertaining to the registration of the Trademark.

As per section 2(1) (m) of The Trademark Act 1999 [7] term 'name' is defined and second-level domain which is the unique name of the company can be included in the purview of this section and making it registrable as per the act.[8] The registration of domain names in India is regulated on a first-come, first-served basis by Domain Name Registrars (DNRs). This means that a domain name, even if it incorporates a well-known trademark, will be registered to the first applicant without considering whether the domain name conflicts with an existing registered trademark. Given that both trademarks and domain names serve the purpose of identifying the products and services of business entities, this approach is leading to potential conflicts between trademark rights and domain name registrations. [9] This is completely ambiguous and gives ample opportunity to anyone to register a domain in the name of a well-known trademarks. This issue came into light when this loop was utilized for fraudulent activities and the matter came before the courts. Considering all the flaws which are prevailing with respect to the registration of the Domain Name. The Supreme Court of India has stated the concern that there is no specific legislation in India to regulate the disputes pertaining the domain name registrations involving well-known trademarks. The court has emphasized that a domain name inculcates all the features of a trademark, and they can be regulated as per the Trademark Act, and they are protected to the minimum extent of passing off.[10]

DNRs are the companies which provide the domain name to the person or the entity to promote their product and services on the online platform. Domain name is mnemonic of the IP address, and this address is a string of numbers in four sets separated by the period commonly known as website.[11] For the process of the registration, one must look up the availability of the combination of words and have liberty to choose a desired name which is second-level

domain.[12] It is an automated process of the registration without any manual intervention or human element to assess the legitimacy of the proposed domain name. DNRs regulate the whole registration process, and a fee has been charged from the registrant while undertaking all his relevant information.[13]Due to the absence of clear regulations with respect to the registration of the Domain Names DNRs are providing alternative domain names knowing the fact that aspiring registrant is applying for the preexisting Domain Name. Registrants are charged a higher price for the registration purpose to get a similar domain name which is in high demand, DNRs are offering such services to make more commercial profits. DNRs are allegedly infringing well-known domain names while following such registration practices. This is resulting in enormous damage to the innocent public who will believe that the website belongs to the actual brand owner. Initially, these websites were being operated by the person who intends to indulge in fraudulent activities like offering distributorships, franchises, dealerships and collecting large sum of money.

DNRs viz-a-viz "Intermediaries" under Information Technology Act

In the emerging landscape of the digital realm, DNRs are evolving as the Intermediaries as these entities are working for the registering and managing the domain names in parallel to the role of the Intermediaries. There were several ambiguities pertaining to the recognition of the DNRs as the intermediaries. IT Act, 2000 acknowledges the intermediaries as network service provider, an information carrier or information publisher.[14]Its basic attribute can be understood with respect to the electronic record as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to the record. They act as a facilitator of electronic messages between the originator and addressee. While referring to the definition of "Intermediaries" provided under section 2(1)(w) of the IT Act, 2000[15] there, we have a term Network Service Provider which is now ever expanding. Also, a similarity can be drawn between the term electronic record and the domain names. As per Section 2(1)(t) of IT Act 2000 "an electronic record" includes the audio, video, data, text or multimedia files generated, stored, received or sent in an electronic form or microfilm or computer-generated micro fiche.[16]To get a better preview of this definition we must refer to the definition of "data" and "information" and "electronic form" defined under section 2(1)(o), Section 2(1)(v) and Section 2(1)(r) respectively.

In the case of the Snapdeal Private Limited v. GoDaddy Com LLC,[17] the Delhi high court has given a clear definition of the Intermediaries while specifically stating that DNRs are the Intermediaries under the IT Act, 2000. In this decision, the court has clarified with a clear interpretation that domain names qualify as "electronic records," particularly because they are issued by Domain Name Registrars (DNRs) from a shared Domain Name Registry. Any entity involved in domain name registration services is thus considered an intermediary under section 2(1)(w) of the IT Act, 2000. Taking this decision into consideration now these DNRs are mandated to work in accordance with the Information Technology Act. This also obligate them to strictly comply with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, (IT Rules, 2021)[18] by the DNRs providing the services in the Indian market.

Due to surge in these matters, it is high time to acknowledge DNRs as Intermediaries. DNRs which were not having their physical presence in India were not ready to comply with the rules and regulation and the court orders of the country. Now DNRs are directed to appoint a Grievance Officer as per Rule 3(2)(a) of IT Rules, 2021. Further this rule mandates that whenever any complaint is made by any user pertaining to any issue that complaint must be acknowledged within 24 h and disposed of in 15 days (about 2 weeks).[19] Grievance officer would be facilitating in compliance of the order by any court or any notice or direction by the government or the competent authority. The Ministry of Electronics and Information Technology (MeitY) is directed to take action against Domain Name Registrars (DNRs) providing domain registration, hosting, and related services within the country if they fail to comply with Indian laws or disregards the courts orders. This has led to a curb in the registration of the Fake Domain Names.

The Masking Dilemma in Domain Name Registration

Registration of domain names has gained a ramp due to the evolution in the digital market. Considering

this surge, international organizations dealing with regulations of global internet has issued several guidelines pertaining to the registration processes. In November 2017 ICANN, the global body to regulate the registration of the DNRs has issued a statement to the registries and the registrars to comply with European Union's General Data Protection Regulation "(GDPR)".[20] This regulation heavily emphasizes the privacy of the personal data such as name, address, email, phone number and other technical and administrative contacts which is collected from the registrant for the identification purpose by the DNRs and this data is also addressed as WHOIS data. Under the garb of this regulation DNRs are providing a privacy protect feature to the registrants in the absence of statutory prescriptions an extra fee has been charged for the same. In consideration of international regulations and local laws, DNRs offer privacy services or brokerage to protect the personal information of registrants or customers from the public disclosure.

The issue came into light when this feature was misused and gave a rise to a new set of issues to the government agencies and the courts as well. In the absence of any regulation pertaining to the registration of domain names, numerous deceptive or misleading domain names have been registered, often exploiting the names of well-known brands. This practice, commonly referred to as cybersquatting, involves registering domain names that are identical or confusingly similar to established trademarks, with an intent to deceive or make profit from the goodwill of those brands. As a result, we frequently encounter websites such as *amazonprize.com*, *tatarecruitment.net*, *kfcfrenchie.com*, and many more. These are fraudulent websites deliberately designed to appear legitimate, exploiting the goodwill associated with reputed trademarks. These fraudulent domains were offering distributorships, franchises, and dealerships to unsuspecting customers, under which an exorbitant amount was collected by them. Once the payment was received, they would take down the domain. They often lure unsuspecting individuals by promising lucrative offers, fake recruitment opportunities, or unauthorized dealership agreements The innocent public, particularly those unfamiliar with the nuances of distinguishing legitimate websites from fraudulent ones, fall prey to these scams, leading to financial losses and breaches of trust. When the matter came to the law enforcement agencies, and they conducted the investigation, they failed to find the suspect as the domain registrant opted for the privacy protect feature, his identity is been masked from the public domain. Investigating agencies further asked the DNRs to disclose their identity and they took the stand that registrant have opted for the privacy protect feature and they are complying with the privacy law of the country, and they are also bound to follow the international regulation.

National Internet Exchange of India "(NIXI)" a nonprofit company which works as facilitators for the improvising of the internet services in India has an agreement with DNRs for the operation of their services in the country.[21] To regulate the market operation NIXI and DNRs which are operating within or from outside the country have signed Registrar Accreditation Agreements "(RAA)", under which mandate all the DNRs to share the WHOIS data with NIXI.[22] The DNRs which are operating in the territory of India are bound to disclose the WHOIS data on the court orders. If DNR is not having a physical presence in India then they are not bound by the RAA agreement and not bound to follow Indian law as well as court orders and they are taking the shade of Right to Privacy and GDPR regulation not to disclose the registrant's data. This whole scenario is evolving as a hurdle to the investigating agencies and to the court as well because without the registrant information, it was a tough task to identify the real culprit and a loop was utilized for the fraudulent activities in blatant manner.

Comparative Analysis of DNR Regulations in United States of America (US) and European Union (EU) Highlighting the Role of Global Organizations

Regulation of DNRs is evolving as a global issue. Several developed nations are struggling with these issues, and they have addressed such issues by reforming their laws in due course of time. The very origin of the issue is when a fraudulent domain application gets accepted by the DNRs, to curb such activities these countries have developed the system for the detection of the application of the abusive domain names. With a strict monitoring technique, it can be easily found that if registrant is applying for the pre-existing well known domain. The process of monitoring is completely based on advanced algorithmic Artificial Intelligence "(AI)". Once detection is made then further verification is done under human supervision to ensure the accuracy of

the results. Since the fraudulent domain name registration is posing a serious concern to all over the globe and it need to be addressed by formulating the effective policy at global level. It is evolving as hurdle to the regulation of product and service through the online platform. US has already adopted the adequate framework to deal with such issues. While EU have also addressed the issues with the several mechanisms to curb the misuse while taking the compliance of the privacy laws into consideration.

US

Anti-cybersquatting Consumer Protection Act' "(ACPA)" was enacted by the US in 1999 with an intend to protect the product and services offered through the domain names on online platform[23]. This legislation keeps a strict eye on the registration of the abusive domain with bad intention or to commit cyber-crime. US completely prohibits the proxy or private registration whereas registry Neustar has developed algorithmic base AI systems to detect international registration of anonymous domain.[24] A frequent check is run through the databases in case of detection of the proxy registration. The concerned registrars are supposed to correct the WHOIS record within 15 days (about 2 weeks).[25] With a parallel check if ambiguous registrations are deleted then as per the agreement if DNRs fails to meet the terms a strict sanction is been imposed on them. These policies are being monitored by the higher official and it allows the investigating agencies to access the WHOIS details in case of fraudulent activities. The US has adopted 'acceptable use policy' which clearly says that if any domain is used for the illegal activities including the infringement of intellectual property right would be taken down while disqualifying the registrant or its agent from any further operation.[26] With the help of these policies all possible measures are been taken to curb the illegal activities carried out through abusive domain names.

EU

Considering the strict privacy regulations, EU have developed their system in such a manner that in the very stage of the registration, if any application has been made for pre-existing domain can be traced. Online criminals often use the authentic contact details for the registration process to ensure the correct identity of the registrant they have adopted 'Know Your Customer "(KYC)" policy.[27] The registrant is bound to produce the authentic identity in the registration process for the verification purpose. Abuse Prediction and Early Warning System "(APEWS)" has been developed by EURid in collaboration with European Union Intellectual Property Office "(EUIPO)" which is trained with immense data for the detection purpose.[28] It works as an 'alert system' for the "(.eu)" domain names under which the holder of trademark will receive the alert when an application is been made for the identical trade mark. This is a free service provided to the (EUTM) European Union trademark holders so that they will be informed before speculative and abusive registration so that they can take the appropriate action in due course of time.[29]A regular screening has been conducted by the system while re-verifying the registrant information at regular intervals of time. The development and the maintenance are being designed in such way that it doesn't give any loop to the criminal to adjust their tactics to bypass the AI detection system. The EU also has a collaborative system with the International Anti-Counterfeiting Coalition "(IACC)" to ensure that they can monitor their DNR registration process globally.[30] There is a statistical exchange of data between the organizations to maintain transparency and to monitor the fraudulent activity effectively. The alert mechanism is an effective policy which may be adopted globally to stop the fraudulent registration of the domain names at the primary stage only.

Role of Global Organizations

ICANN the global organization, working to secure and regulate the domain name registration and the security threats in its study suggests that maximum illegal activities were performed through the domains which were registered via privacy protect services.[31] This privacy protection feature offered as bundle of services to the registrants need clear regulation. When DNRs were asked to disclose the WHOIS data to investigating agencies even on court orders they denied the same quoting the privacy laws and the EU GDPR regulations. But the Government Advisory Committee of ICANN has asked DNRs to give reasonable access of WHOIS data to the law enforcement agencies, for the purpose of investigation when any criminal activity has been done by the Domain. Considering the struggle of privacy protect feature offered by the DNRs under the garb of the GDPR is to secure the data of the registrant from the public domain but it does not restrain the registrars

from sharing that data to the concerned authorities upon the demonstration of specific interest.[32] Domain name dispute is now evolving as the global issue keeping this into consideration Specification 11 of ICANN's Registry Agreement obliges the registry operators to include a provision in their agreement with the registrars prohibiting them from IP infringement and deceptive and fraudulent activates or any other activates that is contrary to applicable laws.[33] Noncompliance with the term of the agreement would amount to the suspension of domain name.

To deal with the issues of registration of the abusive domain names NIXI has Registrar-Accreditation Agreement (RAA) with 171 registrars with respect to the registration of .in "(dot.in)" and .bharat "(dot.bharat)" domain name. The cluse 4.4.3 of the agreement completely puts a bar on the registrars to accept anonymous and proxy registration and registrants cannot avail the privacy protect feature on it.[34] Following the implementation of GDPR, NIXI has masked registrant details to protect their privacy. Whereas upon the direction of the any governmental authority or law enforcement agency or the order of the Court the said details are provided by the NIXI. The regulation of generic top-level domain (gTLD) such as "(.com)", "(.net)" and "(.org)" domain name registration is monitored by the ICANN. The DNRs who provide gTLD have RAA with ICANN and it mandates them strictly comply with the terms of the agreements. As per the section 5.5.2.1.4 of the RAA, ICANN has the authority to terminate a registrar's RAA if a court of competent jurisdiction finds that the registrar has failed to comply with a court order concerning the use of domain names it sponsors.[35] Upon receiving such evidence, ICANN Contractual Compliance will follow its established process to enforce the RAA. Enforcement actions may vary, as the RAA offers multiple remedies, with termination being just one of the possible options. Whereas the clause 3.1 of this agreement gives the clear direction to the DNRs to address the direction of the governmental or semi-governmental authorities promptly and they are abided by the all the applicable laws and regulation of the country they are operating. Clause 3.5, in conjunction with Clause 3.10 of the RRA, requires DNRs to provide complete data to the registry and to comply with ICANN standards in accordance with the Registry Agreement "(RA)".

Registry Agreement bars the registration of reserved names provided by the schedule under Clause 2.6 read with Specification 5 within TLDs, without the expressed permission of ICANN. It puts an obligation on the DNRs to curb the illegal activities. Clause 2.8, in conjunction with Specification 7 of the Registry Agreement (RA), stipulates that the legal rights of third parties must be protected. The Registry Operator is required to take reasonable steps to investigate and promptly address any reports of illegal conduct from law enforcement and government agencies. Specification 6, clause 4 clearly mentions about the Abuse Mitigation while directing the Registry Operators to provide accurate contact details including a valid email address to ICANN and same should be published on their websites. This will help to handle the reports related to the malicious conduct in the top-level domain "(TLD)" and Domain Name System "(DNS)" abuse. Clause 4.2 of Specification 6 mentions the clear guidelines for the DNS abuse mitigation where Registry Operators are directed to take appropriate mitigation actions against the registered domain name in TLD which is being used for the DNS abuse, on the basis of actionable evidence.[36]

ICANN is constantly working to stringent the regulation of Domain Names and curb the DNS abuse. Governmental Advisory Committee "(GAC)" of ICANN issued a policy on DNS Abuse Mitigation which aimed to raise awareness, address the deficiencies and develop relevant and effective abuse mitigation capabilities.[37] The Security and Stability Advisory Committee (SSAC) of ICANN published a report on an Interoperable Approach to Addressing Abuse Handling in the DNS to demonstrate the need for best practices in handling the DNS abuse. The misuse of domain names is undermining the trust in the internet, while affecting the users and service providers, this report proposes a framework to enhance the response to DNS abuse incidents and suggesting prevention and mitigation mechanism in future work.[38] Domain Abuse Activity Reporting (DAAR) project by the ICANN works on to track and analyze the DNS security threats using the data from Reputation Block Lists (RBLs) and focuses on identifying phishing, malware, botnet command and control domains, and spam activities. A monthly report is been published by the ICANN since 2018 while addressing trends related to these threats.[39] On the basis of data collected by DAAR in four years reports starting from 2018 to 2022, ICANN have published a report on DNS abuse. This report underscores the need for cautious interpretation of

DNS abuse trends to avoid misleading conclusions derived from limited dataset[40]. On 11th March 2023 ICANN76 GAC LAC capacity development workshop was held where the issues regarding the DNS abuse in the current trends and future steps to be taken to curb the issue were discussed by the experts of the ICANN.[41] On 5th October 2023 ICANN contracted parties propose the DNS abuse amendment targeting to stop the abuse of gTLD domains while obligating registrars and registry operators to take prompt and appropriate action to mitigate the abuse of DNS. This amendment was been approved by the parties on 13th December 2023.[42] On 5th April 2024 ICANN issued the advisory to ensure the compliance of DNS abuse obligation in Registrar Accreditation Agreement and the Registry Agreement. It mandated the registrars and registry operators in case of ICANN Contractual Complain investigation to provide all the evidences clearly demonstrating the compliance of relevant requirements of these agreements. [43] These regulations will curb the misuse of domain name globally.

Proposals for Legal Reform in India

The 21st century is transformed as the Information Technology century and India is evolving as global IT hub. Every IT-enabled service "(ITES)", e-commerce (online business), social media platforms are eager to provide their services in the country. To regulate these services efficiently India, need to reform their laws. Issues like cybersquatting are very new to the Indian digital space due to lack in the digital literacy. Domain Names have gained an effective acknowledgement in the Indian market and the recognition under the Trademark Act, everyone wants to promote their product and services on online platform. In the absence of effective regulations of DNRs, leaves an ample space for fraudulent activities as Trademark Act does no suffices clear registration process and other regulations. The Supreme Court has already drawn a similarity between the domain name and the trademarks, [44] but Indian legislation is still silent to give a clear framework in this regard.

The registration and technical handling of the Domain Names is completely in the hands of DNRs. The ambiguous registration techniques and offering of the privacy protect feature have so many discrepancies altogether. DNRs which were operating from outside the county without having any physical presence in India were not ready to comply with the local laws of the country and court orders. But DNRs are not immune to liability anymore as they have been acknowledged as the Intermediaries under the IT Act, 2000. They are making huge revenue from the Indian market it creates the strict obligation on them to comply with the Indian laws if they want to provide their services in the Indian market.

For more effective supervision of misuse of domain name from IP- infringing activities government should adopt the policy of good practice under which the screening of the domain names would be done in three stages: Pre- registration, Registration, and Post Registration. At the pre-registration stage registries will set the detailed terms and conditions while including IPR infringement activity as breach of law and contractual terms amounting to the suspension of domain name. At this stage the alert system can be adopted where trademark holders get notified in case there is any resemblance in the application of domain name registration with their trademark. To trace the potential abusive registration AI algorithms can be employed to analyze the pre- registration data based on keyword or patterns and flagging them for the immediate action. In registration stage registries must verify that the data provided by the registrant is correct while updating it on regular basis which will help in crosschecking the fraudulent registration consequently blocking them. The (KYC) Know Your Customer policies can give an effective way to validate the identity of the registrants. The personal data collected from it can be used to develop the advance monitoring and abuse prediction systems. With the help of these systems potential misuse of the domain can be predicted and verified before delegation. There must be a limit on number of domain names as per individuals or organizations which will reduce the registration of abusive domain by the malicious registrants. Finally in post registration a manual and automated verification of WHOIS data can be done and the domain who fails to prove their identities must be suspended. The fraudulent registrants often use false and unverifiable details during registration process. In such scenario Registries should collaborate with the law enforcement agencies and implement the (NTD) Notice and Takedown mechanisms where suspended and flagged domains require additional verification and legitimate evidence before reactivation.

The harm caused to both consumers and businesses highlights the pressing need for the enactment of

appropriate regulations. Contours of such regulatory framework need to be based on certain principles. Intermediary exemption should not be available when the DNRs are doing it for commercial gains. Absence of exemption will pave way for better data sharing and evidence collection leading to proper enforcement. For masking services, there can be distinction between commercial and non-commercial work of the website and harm to consumer need to be addressed and proper remedies should be provided. This issue is evolving with the new digital realms which are coming up with time. Considering all these discrepancies in the legal framework, legislative authorities should take charge to come up with clear guidelines to address these issues

India needs a similar framework which US and EU have as they are monitoring the registration of the registration of the Domains and the proper identity verification of the registrant before delegation of the domain name to the registrant. Legislative bodies must come up with a separate act to regulate the registration of the domain in an elaborative manner and to address cybersquatting issues. Ministry of Electronics and Information Technology "(MeitY)" must come up with strict guidelines to appoint Grievance Officer by every DNRs and ensure they are complying with the Indian laws and court orders. Such mechanisms will ensure a safe digital environment and put a curb on cybersquatting issues.

Conclusion

Domain names have attained overwhelming support and widespread adoption in the global digital space. In India, the existing laws addressing digital issues are inadequate in effectively tackling challenges like cybersquatting, as such concerns remain largely unaddressed in legislative enactments, whether fully or partially. This serves as a wake-up call for policymakers to take immediate action and implement comprehensive legal frameworks to curb these issues. The Indian digital ecosystem is expanding rapidly due to the constant surge in population, coupled with the availability of low-cost computing and connectivity. On the other hand, the absence of efficient digital education to equip users with the necessary skills to navigate this evolving landscape is exacerbating the situation. Considering the global struggle in addressing the issues highlighted above emphasize the growing threats posed by deceptive and fraudulent domain names, which are eroding public trust in the digital ecosystem worldwide. The root cause of this issue lies in the registration of misleading and fake domains by DNRs and enabling the unchecked and questionable practices surrounding these domains under the garb of privacy protect features despite the various global guidelines formulated by ICANN. A significant challenge in addressing this global problem is the lack of strict enforcement, as compliance of regulations remains largely voluntary by DNRs. The absence of stringent and coercive measures against non-compliance has further aggravated the situation. Global domain regulatory authorities need to deliberate on the strict implementation of existing frameworks while also addressing ongoing and emerging challenges in domain name disputes occurring worldwide. Strengthening enforcement mechanisms and adapting regulations to evolving digital threats will be crucial in ensuring a more secure and trustworthy domain name system.

References

1 Candela M, Luconi V, Vecchio A. Impact of the COVID-19 pandemic on the Internet latency: A large-scale study. *Computer Network,* 182 (2020) 5.

2 Creasman W, Establishing geographic rights in trademarks based on internet use*,* The *Trademark Reporter*, 95 (2005) 1016–17.

3 Weiswasser G, Domain Names, The internet, and trademarks: Infringement in cyberspace, *The Santa Clara High Technology Law Journal, 20* (2003) 215.

4 The IP number is of Maharashtra National Law University, Aurangabad website.

5 Arnot J, Navigating Cybersquatting Enforcement in the Expanding Internet, *John Marshall Review of Intellectual Property Law,* 13 (2014) 321.

6 ICANN History Project, ICANN, https://www.icann.org/history (accessed on 28 October 2024).

7 Act, The Trademarks Act, 1999, (Act No. 47 of 1999), Government of India, 1999, Section 2(1) (m)

8 *Living Media India Limited v. News-aajtak.co.in*, (2023) SCC OnLine (Del) 7368.

9 Policies, Ernet-India, https://registry.ernet.in/Policy.aspx. (accessed on 28 October 2024).

10 *Satyam Infoway Ltd.* v *Sifynet Solutions Pvt. Ltd.*, (2004) 6 SCC 145.

11 McGrady, Drinking from a fire hose: Future-proofing your internet strategies, *World Trademark Review,* 41 (2013) 79.

12 Levy J, The confusion of trademark territoriality, *UIC Review of Intellectual Property Law,* 18 (2019) 324.

13 Abel S, Trademark issues in cyberspace: The brave new frontier, *Michigan Telecommunications and Technology Law Review,* 5 (1999) 4.

14 Gupta A and Sapre A, *Commentary on information technology act with rules, regulations, orders, guidelines, reports and policy documents* (Lexis Nexis Delhi) 2015,75

15 Act, The Information Technology Act, 2000, (Act No. 21 of 2000) Government of India, 2000, Section 2(1)(w)

16 Nappinai N, *Technology Laws Decoded Hardcover* (Lexis Nexis Delhi) 2017,205
17 *Snapdeal Private Limited* v *GoDaddy Com LLC*, (2022) SCC OnLine Del 2044.
18 The Information Technology (Intermediary guidelines and Digital Media Ethics Code) Rules, 2021.
19 *Dabur India Ltd.* v *Ashok Kumar,* (2022) SCC OnLine Del 2911.
20 Guidelines for Proposed Models to Address the General Data Protection Regulation (GDPR), ICANN (2017), https://www.icann.org/resources/pages/gdpr-proposed-models-guidelines-2017-12-08-en. (accessed on 28 October 2024).
21 NIXI | Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/content/nixi. (accessed on 28 October 2024).
22 Registrar Accreditation Agreement (RAA) & Related Materials - ICANN (n.d.). https://www.icann.org/resources/pages/registrars/registrars-en. (accessed on 28 October 2024).
23 Mota S, The anti cybersquatting consumer protection act: An analysis of the decisions from the Courts of Appeals, *UIC John Marshall Journal of Information Technology & Privacy Law*, 21 (2003) 355.
24 The future of internet navigation and the domain name system, An invitation to individuals worldwide to provide input to a study conducted by the U.S. National Academy of Sciences, http://www7.nationalacademies.org/cstb/project_dns_input.html. (accessed on 28 October 2024).
25 The Popularity and Importance of Search Engines, Data Memo, Pew Internet & American Life Project (Aug.) http://www.pewinternet.org/pdfs/PIP_Data_Memo_Searchengines.pdf. (accessed on 28 October 2024).
26 Acceptable Use Policy, .US Domains, https://www.about.us/documents/policies/usTLD_Acceptable_Use_Policy.pdf (accessed on 28 October 2024).
27 Domain names discussion Paper Observatory, https://euipo.europa.eu/ohimportal/en/web/observatory/-/news/domain-names-discussion-paper. (accessed on 28 October 2024).
28 1st AI-driven proactive suspension system for domain names, More News EURid, https://eurid.eu/en/news/1st-ai-suspension-system-for-ds/. (accessed on 28 October 2024).
29 Study on evaluation of practices for combating speculative and abusive domain name registrations, https://op.europa.eu/en/publication-detail/-/publication/e88d02f9-cbc6-11ea adf701aa75ed71a1/language-en. (accessed on 28 October 2024).
30 Europol Global Anti-Counterfeiting Authorities Gather at 2nd Annual Europol Intellectual Property Crime Conference Europol, https://www.europol.europa.eu/media-press/newsroom/news/global-anti-counterfeiting-authorities-gather-2nd-annual-europol-intellectual-property-crime-conference. (accessed on 28 October 2024).
31 Study on whois privacy & proxy service abuse, ICANN, https://www.icann.org/en/public-comment/proceeding/study-on-whois-privacy--proxy-service-abuse-24-09-2013. (accessed on 28 October 2024).
32 Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement,https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2021_Discussion_Paper_on_Domain_Names/2021_Discussion_Paper_on_Domain_Names_FullR_en.pd (accessed on 28 October 2024).
33 Base Registry Agreement, ICANN, https://www.icann.org/en/registry-agreements/base-agreement, (accessed on 28 October 2024).
34 Registrar-Accreditation Agreement (RAA). NIXI https://registry.in/system/files/RAA_28042022.pdf (accessed on 28 October 2024).
35 "Registrar Accreditation Agreement (RAA) & Related Materials - ICANN" <https://www.icann.org/resources/pages/registrars/registrars-en> (accessed on 28 October 2024).
36 "Base Registry Agreement" https://www.icann.org/en/registry-agreements/base-agreement (accessed on 28 October 2024).
37 DNS Abuse Mitigation, ICANN.org (2019), https://gac.icann.org/activity/dns-abuse-mitigation (accessed on 28 October 2024).
38 ICANN Security and Stability Advisory Committee (SSAC), (2021) <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf> (accessed on 28 October 2024).
39 Domain Abuse Activity Reporting - ICANN, Icann.org (2017), https://www.icann.org/octo-ssr/daar (accessed on 28 October 2024).
40 ICANN, DNS Security Threat Mitigation Program, Tajalizadehkhoob S & Weinstein R, The Last Four Years in Retrospect: A Brief Review of DNS Abuse Trends (2022) <https://www.icann.org/en/system/files/files/last-four-years-retrospect-brief-review-dns-abuse-trends-22mar22-en.pdf> (accessed on 28 October 2024).
41 ICANN76 GAC LAC Capacity Development Workshop - DNS Abuse (2/4), Icann.org (2023), https://gac.icann.org/sessions/icann76-gac-lac-capacity-development-workshop-dns-abuse-2-4 (accessed on 28 October 2024). https://www.icann.org/en/blogs/details/icanns-contracted-parties-approve-new-obligations-to-mitigate-dns-abuse-13-12-2023-en (accessed on 28 October 2024).
42 "ICANN's Contracted Parties Approve New Obligations to Mitigate DNS Abuse" (2023) https://www.icann.org/en/blogs/details/icanns-contracted-parties-approve-new-obligations-to-mitigate-dns-abuse-13-12-2023-en (accessed on 28 October 2024).
43 *Satyam Infoway Ltd* v *Sifynet Solutions Pvt Ltd*, (2004) 6 SCC 145.