The burgeoning of fraud by infringing domain names with hidden or incorrect WHOIS data. Where does the liability lie?

Thought Leadership • January 31, 2021
This article was first published in the 31st January 2021 edition of Asia IP Magazine.
Authors: Saif Khan and Shobhit Agrawal

Since the advent of the internet, a domain name has practically served as the first point of contact for a potential customer of any business. A domain name can be registered by anyone upon payment of the applicable fee and furnishing basic contact information. This information then forms part of the domain's WHOIS record, part of a collection of databases run by registrars and registries around the world. The process of allotment of a domain has been on a first-come-first-serve basis, with no real responsibility on anyone towards legitimacy or correctness of allotment of a particular domain to an applicant. Consequently, it has always been easy for anyone to indulge in cybersquatting, simply obtaining a domain name comprising someone else's trademark (or even personal name) without any legal or procedural hurdles, so long as the particular domain is available for registration.

WHOIS database management is administered by the ICANN and is intended to make the information about websites and their owners accessible so as to enable resolution of disputes relating to them. However, the lack of any sanctity, legal obligation or even a basic gatekeeping of the contact information furnished by the domain registrant has enabled the squatting of (infringing) domain names to be an extremely easy and literally risk-free exercise. Resultantly, the WHOIS data has become meaningless in many, if not most, cases of dishonest domain registration, as it fails to identify the actual registrant of an unscrupulous domain, thereby disabling right owners to take legal remedies as they cannot ascertain the actual identity of the wrongdoer. The eventual fallout is that internet frauds continue to increase with ever increasing pace, aided by faster and more accessible internet, rising technology literacy and, most crucially, the availability of an almost-absolute anonymity, providing an in-built shield against any swift legal actions or consequences.

A liability-free infringement and fraudulent activities breeding ground?

Unlawful acts of such a nature and extent surely cannot be free from any legal remedies, as any prudent person would imagine. The actual situation, unfortunately, is largely to the contrary, and cybersquatters are freely and openly thriving by misusing the anonymous nature of the cyber world to their advantage as a breeding ground to illegally earn a quick buck and yet be scot-free when it comes to any consequences.

As of the writing of this article, the Delhi High Court is facing perhaps the largest volume of such disputes in the court's history, replete with litigation by brand owners complaining of registration of a series of infringing domain names by unknown people which are used for frauds like employment scams, fake franchisee/distributorship offers, illegitimate lucky draws and the like. The common pattern in all such cases is that the identity of the domain registrant is unknown because it is false and/or hidden. Consequently, there remains no option for a plaintiff but to necessarily array the domain registrar(s) as a defendant in the suit. The registrar, however, will almost certainly claim a safe harbour position of intermediary in such actions and escape any other liability apart from blocking the offending domains.

Domain registrars also resist injunctions against the future issuance of domain names under a particular trademark, taking a common stand that, firstly, the transaction is not in their control as it is an automated process, and, secondly, that it is impossible for domain registrars to monitor each individual domain in a space spanning millions of domains. Furthermore, the domain registrars assert that they are neither an appropriate entity nor are they equipped to determine whether a particular domain causes an infringement of someone's trademark rights.

While each of the above stands can be fairly understood and conceded to, in the view of the authors, the crux of the issue revolves at the Registrar's disinclination at performing a basic mandatory due diligence as to the identity of the domain registrants, or what is commonly termed as a Know Your Customer (KYC) record. It cannot be denied that, after all, the registrars offer their services of registration of domain for profit/fee as well as that the scope of misuse of a domain name is vast, in both extent and territorial reach. Therefore, a complete absence of any kind of due diligence towards the identity of a domain registrant is not only surprising but also the need of the hour. Hence, mandating the domain registrar with the task of securing a basic KYC record of each domain registrant to begin with, which certainly can be through an automated process as is commonly exercised by various institutions, shall be able to significantly reduce the time in identifying the culprits of cybersquatting for fraudulent activities. Such a practice also secures the interests of domain registrars as the right holders can then go after the real culprits without necessarily dragging domain registrars to legal actions.

Moreover, national domain management authorities, like the National Internet Exchange of India (NIXI) in the case of India, must also take the initiative to frame policies so that the domains under their jurisdiction – i.e., the .in domains – are issued in compliance with strict KYC requirements considering the increasing domain/internet frauds emanating from India. This is especially imperative due to the repeated stands taken by the domain registrars that they are not mandated by any law or rule to conduct any KYC due diligence for domain registrations. There exists an imminent need for all stakeholders to collaborate and come up with a domain name framework that ensures that both private rights and public interests are secured. If steps are not taken by stakeholders, there could be a serious problem for courts and law enforcement to deal with the issue effectively due to

the huge number of cases, the real victims of which are almost always the general innocent public at large.