COMMENTARY

UDRP: Still a Powerful and Efficient Tool for Combatting Anonymous Cybersquatters

While it is always preferable to prevent cybersquatting by registering all of the relevant domain names and variations a business may need, UDRP continues to serve as a powerful and efficient tool for IP owners stop cybersquatters and protect their business's goodwill.

March 19, 2023 at 01:47 PM

Special Sections

By Kate Sherlock | March 19, 2023 at 01:47 PM

The Anti-Cybersquatting Consumer Protection Act (ACPA) defines cybersquatting (domain squatting or domain hijacking) as registering in, trafficking in, or using an internet domain name with a bad faith intent to profit from the goodwill of a trademark or service mark belonging to someone else. See 15 U.S.C. Section 1125(d). Cybersquatting comes in many different forms. There is "typo-squatting" or "domain spoofing," where a bad actor registers a domain name with a slight change or typo (think goooogle.com versus google.com or amazom.com versus amazon.com). Often, these bad actors advertise similar services and profit from third-party links on their site. In more serious cases, they copy copyrighted content from the legitimate website to trick visitors into purchasing goods or services from their fraudulent site and/or submitting personal information as part of a larger scam. Cybersquatters may also register variations of well-known trademarks in an effort to sell the domain variations back to the trademark owner at a high mark-up.

Prior to the European Union's adoption of the General Data Protection Regulation (GDPR), it was easier for trademark owners to identify and combat cybersquatters. Pre-GDPR, anyone could run a free WHOIS search to identify contact information for a domain registrant, including their name, mailing address and email address. WHHOIS is a public database regulated by the Internet Corporation for Assigned Names and Numbers (ICANN) that stores domain registrant information. Once the relevant registrant was identified, trademark owners could pursue a variety of legal options, from sending a cease and desist letter directly to the domain registrant to initiating federal litigation under the ACPA. But, when GDPR went into effect on May 25, 2018, many domain registrars stopped publicly displaying registrant information because doing so is at odds with GDPR, which aims to protect European Union citizens' privacy by imposing certain restrictions on data collectors and processors. Due to its extraterritorial application and the uncertainty surrounding its scope, many registrars erred on the side of caution and removed all registrant information rather than tailoring their removal to EU personal data. Now, a WHOIS search returns only the state or province and country for natural persons and an anonymized email address, rather than a true email address, for domain registrants. Almost overnight, WHOIS transformed from the de facto source for domain registrant information to a rarely helpful search tool.

GDPR has had far-reaching positive effects to protect individuals' privacy, but it has also had the unintended consequen ce of assisting cybersquatters in maintaining their anonymity and increasing enforcement costs for IP owners. Acknowledging the tension between complying with privacy laws while assisting IP owners in protecting their assets, ICANN mandated that ICANN-accredited registrars provide third parties with reasonable access to personal

data of registrants if they have a “legitimate interest” as defined under GDPR, except where such legitimate interest is overridden by the interests or fundamental rights and freedoms of the data subject pursuant to Article 6(1)(f) GDPR. But, nearly five years after GDPR went into effect, there is no standardized approach for requesting non-public registrant information from a registrar. Many registrars have adopted their own procedure for submitting such requests, with some registrars like Go Daddy requiring that requestors exhaust other “less-intrusive mechanisms” prior to requesting nonpublic registrant information.

Fortunately, the Uniform Domain-Name Dispute Resolution Policy (UDRP) provides trademark owners with a cost-effective, quick method for obtaining relief from anonymous cybersquatters. Under the UDRP, the owner of a trademark (either a registered mark or a common law trademark) can seek to cancel or gain control of infringing domains by filing a complaint in a private arbitration proceeding, even if the cybersquatter is located outside of the United States and cannot be identified. All ICANN-accredited registrars who control the registration of domain names are subject to the UDRP, which is why it is such a powerful and efficient tool to combat cybersquatting and protect trademark owners’ rights.

To seek relief under the UDRP, a trademark owner (the complainant) must first file a complaint with a recognized UDRP service provider, such as the Forum or the World Intellectual Property Organization (also known as WIPO). If the registrant of the infringing domain is unknown, the complainant must simply identify the information available to it through a WHOIS search. Once the complaint has been submitted to a UDRP service provider, ICANN-compliant domain registrars provide contact information for the relevant infringing domain and “lock” the domain name’s registration and registrant information so that no changes may be made during the pending UDRP proceeding. The registrar also provides notice to the disputed domain registrant that the UDRP proceeding has been initiated. At that point, the registrant may file an answer in response to the complaint and occasionally, the registrant does not respond.

Once an answer is filed or the deadline to file an answer passes, the dispute resolution provider assigns the case to a single or a three-person administrative panel to consider the filed papers. The complainant has the burden of demonstrating that the disputed domain is identical or confusingly similar to the complainant’s trademark or service mark, that the registrant of the disputed domain has no legitimate interest or rights in the disputed domain, and that the registrant registered the disputed domain in bad faith. If the complainant’s trademark is unregistered, the complainant must set forth additional supporting facts surrounding its trademark use, including duration, sales information, advertising, and customer recognition. If the panel finds that the complainant met its burden by establishing the three elements discussed above, the panel issues a decision in the complainant’s favor and the registrar must, at complainant’s option, either cancel the disputed domain or transfer it to the complainant. Transferring the domain is the preferred option because it prevents the domain from being registered by another bad actor in the future. If the panel decides that the complainant failed to meet its burden, the disputed domain remains with the registrant. Finally, it should be noted that UDRP proceedings can be appealed through a federal lawsuit.

From the filing of a complaint to domain transfer, the entire UDRP process takes approximately 60 days and is, in almost all cases, significantly less expensive than litigation because it involves fewer filings and no formal discovery.

While it is always preferable to prevent cybersquatting by registering all of the relevant domain names and variations a business may need, UDRP continues to serve as a powerful and efficient tool for IP owners stop cybersquatters and protect their business’s goodwill.

Kate Sherlock *is a partner at Archer & Greiner, She has won numerous UDRP actions on behalf of her clients. If you have questions regarding the UDRP process, contact her at ksherlock@archerlaw.com or 856-673-3919.*
