Searchers Beware!

⊕ *The potential perils of performing a WHOIS search*

By **Gretchen M. Olive**, Director of Marketing of Corporation Service Company

IN SUMMARY

– There has been wide speculation over the last couple of years that a practice called 'domain name front running' had been taking place

– Domain name front running is when a party who has some form of insider information regarding an internet user's interest in a domain name pre-emptively registers the name

– On 8 January 2008 various blogs and online domain industry news sources began to report that *Network Solutions* had implemented a policy whereby the registrar itself was registering names that had been searched, but not registered, on their website

AUTHOR

Gretchen M. Olive is Director of Marketing at Corporation Service Company. Over the last seven years she has helped Fortune 500 companies and other business entities devise global domain name and brand protection strategies to protect their IP on the Internet. Gretchen is a member of the Internet Corporation for Assigned Names and Numbers' (ICANN) Registrar Constituency, INTA and the Association of Corporate Counsel (ACC) and speaks internationally on issues related to domain names, trademarks and online brand protection. She was recently appointed to INTA's Registration Practice & DNS Administration Subcommittee of the Internet Committee for the 2008-2010 term.

In January the IP community was once again reminded that policy always lags behind technology. On 8 January 2008 various blogs[1] and online domain industry news sources[2] began to report that Network Solutions (NSI) had implemented a policy whereby the registrar itself was registering names that had been searched, but not registered, on their website, *www.networksolutions.com*.

There has been wide speculation over the last couple of years that a practice called 'domain name front running', had been taking place. Domain name front running is when a party who has some form of insider information regarding an internet user's interest in a domain name pre-emptively registers the name. While documented evidence of this practice had been elusive, industry groups and IP advocates continued to express concern and fear that the frequency of the practice had been growing over the last year. As a result, the ICANN Security and Stability Advisory Committee (SSAC) undertook a review of the alleged practice which led to the release of an Advisory on domain name front running by the SSAC in October 2007[3].

The SSAC based their review on the premise that, "checking the availability of a domain name can be a sensitive act which may disclose an interest in or a value ascribed to a domain name." However, after closely examining numerous allegations and suspected incidents of front running, the SSAC concluded the information supplied was "anecdotal and incomplete". As a result the SSAC called for the IP and internet community to work together to further comment on the issue and to develop standards clearly defining acceptable and unacceptable practices.

With the image of the domain name industry and the interests of internet users across the globe at stake, the SSAC also set out a wish list of information the SSAC believed would help more fully explore and corroborate allegations of domain name front running and asked the internet community at large to send this and other relevant information to them directly[4] for investigation. Suggested evidence set out by the SSAC[5] included:

• Method used to check domain name availability (e.g., web browser, application).
• Local access ISP.
• Provider or operator of the availability checking service.
• Dates and times when domain name availability checks were performed.
• Copy of the information returned (e.g., WHOIS query response) in the response to the availability check.
• Whether the domain name was reported as previously registered or never before registered in the response returned from the availability check.
• Copy of the information returned (e.g., WHOIS query response) indicating the name had been registered.
• Copies of any correspondence sent to or received from the registrant perceived to be a front runner.
• Correspondence with the registrar or availability checking service.
• Any information indicating a potential relationship between the availability checking service and the registrant that grabbed the name.

While the Advisory issued by the SSAC was credited with framing and giving additional credibility to domain name front running allegations, many were disappointed that no declaration was made that front running was indeed happening; and worse, once again ICANN was taking a wait and see stance.

On 8 January 2008, when the news of NSI's new policy of registering domain names for which availability searches were

conducted, but not registered, began to surface, the *TMtopics Discussion List*[6] hosted by the *International Trademark Association* (INTA). Postings quickly began to rush in with example after example of names Internet users had searched on the NSI website, but did not register, which quickly thereafter were found to be registered to NSI as evidenced by the information posted in the Registrant field of the Who is:

> Registrant : Make this info private
> This Domain is available at
> NetworkSolutions.com
> 13681 Sunrise Valley Drive, Suite 300
> Herndon, VA 20171
> US

Concrete proof?

Finally, many thought, concrete proof of front running by one of the largest ICANN-accredited registrars. However, as the SSAC Advisory had warned several months prior[7], nothing in the ICANN Registrar Accreditation Agreement (RAA) expressly prohibited registrars from monitoring and collecting Whois and availability query data and either selling it or using it for its own business purposes. In fact, *Jonathan Nevett, Vice President of Policy at Network Solutions*, quickly sought to vindicate NSI's practices by releasing the following statement through a popular domain industry blog[8]:

> *"I'd like to clarify what we are doing. In response to customer concerns about Domain Name Front Running (domains being registered by someone else just after they have conducted a domain name search), we have implemented a security measure to protect our customers. The measure will kick in when a customer searches for an available domain name at our website, but decides not to purchase the name immediately after conducting the search.*
>
> *After the search ends, we will put the domain name on reserve. During this reservation period, the name is not active and we do not monetize the traffic on these domains. If a customer searches for the domain again during the next 4 days at networksolutions.com, the domain will be available to register. If the domain name is not purchased within 4 days, it will be released back to the registry and will be generally available for registration.*
>
> *This protection measure provides our customers the opportunity to register domains they have previously searched without the fear that the name will be already taken through Front Running.*
>
> *You are correct that we are trying to take an arrow out of the quiver of the tasters. As*

you know, domain tasters are the largest Front Runners. Due to no fault of registrars, Front Runners purchase search data from Internet Service Providers and/or registries and then taste those names. Some folks may not agree with our approach, but we are trying to prevent this malicious activity from impacting our customers."

Despite the fact that NSI was pledging not to monetize the domain name, i.e., not use it to operate a pay-per-click site where NSI would profit, many were sceptical of NSI's motives. Instead of quelling concern, the statement by Mr. Nevett further fuelled debate and many claimed that NSI were forcing them to use NSI to register a name that had been registered as a result of their new practice for a premium price (typically $34.99).

Furthermore, additional concerns were raised about whether a domain name registered as a result of a mere search now had a bounty on it if the name was not ultimately registered within the 5-day add grace period (AGP) that domain name registries like Verisign (registry operator of the .com and .net top-level domains) had in place to allow those who had mis-registered names with wrong spellings to delete the name without cost. Also, many questioned if NSI's motives really achieved the stated goal considering there was no process in place to ensure the person who had searched the name that triggered the registration was the only one who could register it during the period NSI was holding the name.

While NSI has made some subsequent modifications to the implementation of its policy[9], the practice has not discontinued and once again ICANN's effectiveness in proactively developing policies to deal with issues like domain name front-running, domain tasting, domain kiting and other domain system gaming practices is casting a dark shadow on the domain name industry and internet overall. While there have been significant improvements in how ICANN is operated and there have been efforts made to make the entire policy making process more transparent and accessible, it is just too little and it is too slow in light of how rapidly technology forces change.

Domain tasting/kiting

There is a popular phrase that says, "think globally, act locally". As IP holders, as business people, as consumers we need not only to find time and resources to participate in the global policy process, but we have to look at each of these issues as internal business problems for which we need to

determine the root cause and propose a "local" remedy that meets the needs of our business and constituents.

For example, look what Google did. While domain tasting (speculative registration of domain names for less than 5 days to determine if interest in the domain name itself or web traffic generated by the domain name is sufficient to generate enough revenue to justify at least a full year of domain name registration), domain kiting (deleting newly registered domains within the grace period then immediately re-registering them to reset the grace period and postpone payment) and domain front running are different schemes, the motives behind these practices are similar – money, specifically the potential to get a name that can help generate significant pay-per-click revenue for the owner. And no one understands the value of pay-per-click better than Google.

Many familiar with the 'Google AdSense' Domain program know that the program allows domain name owners to sign on with Google and create web sites that contain links that would be relevant to an internet user based on their search criteria or the domain name to which they directly navigated. Once on the site, each time an internet user clicks on one of the links, money is paid to the domain name owner of that website in return for passing a visitor onto one of Google's advertisers. While this program is popular and has given many domainers engaged in the practice of domain tasting and domain kiting an opportunity to make millions without little to no risk because they only have to pay for a name once it has been registered for more than 5 consecutive days, Google has demonstrated with a recent change in policy regarding the AdSense Program that it is taking matters into its own hands to disassociate itself and its popular program from domain kiters.

Specifically, on 25 January 2008 Google announced it would implement a new *"domain kiting detection system"* by February 11th. Little detail has been released on exactly how Google will do this, but in an e-mailed statement[10] Google described, *"If we determine that a domain is being kited, we will not allow Google ads to appear on the site. We believe that this policy will have a positive impact for users and domain purchasers across the Web."* Although Google, has not said they will monitor their client base for domain name tasting, this move by Google clearly demonstrates that Google has looked at the problem affecting the reputation of their program, identified a root cause and has now

proposed a remedy. While this is an extreme example, it is a good one and one that can give guidance and insight to policy makers as they catch-up to the problem.

So, if domain tasting, domain kiting or domain front running is impacting your business, what can you do internally (i.e., locally) to minimise its impact:

- *Find a trusted advisor.* These issue morph and change daily and it is hard to keep up with all the twists and the turns. Identify a partner who understands the space, can keep you apprised of developments that may affect your business and who has the time and resources to understand your business and help you find best practices that can help mitigate the problem for your organisation or client.

- *Find out how people in your organisation and those who work with you in securing brands, trademarks and corporate identities search for availability of these names.* Start with understanding what Whois search tools people are using and publish a list internally of those tools you have verified are operated by those who do not use or sell their Whois and availability search query data.

- *Beat the domain tasters, kiters and front runners to the punch.* Domainers scour and warehouse data either by purchasing it or "scraping" it from all sorts of public and online databases to find ideas for names to register. Public trademark filing data, corporate name reservations and business formation databases are prime targets. Implement processes internally which secure potential brand names, trademarks or other corporate names prior to or simultaneous to using it in a press release announcing a product release, filing for a trademark, forming a new company and registering it with the appropriate government office.

- *Develop and implement a domain name policy.* You are not alone if you work in an organisation where there is no written domain name registration policy. Many organisations are just getting to the point where there is one person, team of people or department responsible for maintaining and managing the company's domain names. Implementation of a written domain name registration policy can help you bring it all together and clearly set expectations as to what names should be registered, how names should be searched, when they should be purchased and who is responsible. This policy can take

significant risk out of a name slipping through the cracks and help reduce enforcement and domain recovery costs because the names you care about will be controlled by you.

- *Get the names the domain tasters, kiters and front runners will register once they learn of your interest in a name.* A recent analysis of 100,000 domain names[11] has confirmed that domainers like names that are cheap and easy to get. As a part of your domain name policy make sure you secure names prior to or simultaneously with whatever trademark filing, corporate name registration or press release you will be issuing. It only takes seconds to register a domain name and the cost is relative compared to trying to get that name back once someone snatches it.

- *Be vigilant and recruit everyone to help you monitor the controls and policies you have implemented to sustain the program you have put in place.* Your domain name registration strategy and protected names should not be a secret. Let everyone within your organisation and among your partners know about your policy and solicit there buy-in, commitment and help. Create an atmosphere where everyone feels like it is their duty to protect the company's names. In addition, don't just solicit help once or make a big splash internally about the implementation of your new domain name policy, be vigilant and look for tools and ways you can monitor its implementation and ways you can integrate this mission to protect your corporate identity into your corporate orientation, on-going employee training program and performance plans.

- *Report wrong doers.* Let others know about the problems and issues you have experienced in managing your company's corporate identities online. Sign-up for *ListServs* or discussion groups that the various trade organisations operate that you belong to and find out if anyone else has experienced the problem. It is likely you can gain valuable insight and suggestions on how to deal with the situations; anything from a specific group or taskforce that is examining the problem, to someone who has a tool that combats that problem to a legislator that is considering legislation. There is strength in numbers and if you keep it a problem a secret its full extent may not be fully realised or any evidence available.

In the end, you will be glad you took action and did not get overwhelmed by the enormity of the issue and politics of the global internet community affecting your IP rights and business. ⊕

Notes

1   Network Solutions steals domain ideas; Confirmed! DomainTools Blog, 8th January, 2008 (http://blog.domaintools.com/2008/01/network-solutions-steals-domain-ideas-confirmed/)

2   Domain Registrar Network Solutions Front Running on Whois Searches, DomainNameNews, January 2008 (http://www.domainnamenews.com/featured/domain-registrar-network-solutions-front-running-on-whois-searches/1359)

3   SAC 022 SSAC Advisory on Domain Name Front Running, October 2007. (http://www.icann.org/committees/security/sac022.pdf)

4   mailto:SSAC-Fellow@ICANN.org

5   Page 10, 022 SSAC Advisory on Domain Name Front Running, October 2007. (http://www.icann.org/committees/security/sac022.pdf)

6   To view or search posting and subscribe to the INTA TMtopics Discussion List, go to: http://www.inta.org/index.php?option=com_content&task=view&id=1397&Itemid=232&getcontent=1

7   See page 8, paragraph 4 of SAC 022 SSAC Advisory on Domain Name Front Running, October 2007. (http://www.icann.org/committees/security/sac022.pdf)

8   See CircleID Blog, January 8, 2008, http://www.circleid.com/posts/81082_network_solutions_front_running/

9   Network Solutions Getting Better, DomianTools Blog, January 15, 2008, http://blog.domaintools.com/2008/01/network-solutions-is-getting-better/

10 Google Takes Aim at Domain Tasting Profiteers, Information Week Online, 25 January 2008 http://www.informationweek.com/news/showArticle.jhtml?articleID=205918984

11 Infringement Trends in the Domain Name Marketplace, available upon request at http://www.cscprotectsbrands.com