



**Comments  
of  
InterContinental Hotels Group  
on  
A Study of Whois Privacy and Proxy Service Abuse  
conducted by the  
National Physical Laboratory  
for the  
Internet Corporation for Assigned Names and Numbers (ICANN)  
October 22, 2013**

InterContinental Hotels Group (IHG) appreciates the opportunity to submit these comments on a Study of Whois Privacy and Proxy Service Abuse submitted to ICANN by the National Physical Laboratory on September 20, 2013. IHG represents 4,150 hotels across nearly 100 countries operating under nine hotel-brand names. Our group's members account for more than 160 million hotel stays in more than 620,000 rooms annually. We are pleased to play an active role in ICANN's ongoing policy dialogue that affects our company, brands, and the business community as a whole.

Internet commerce is a vital part of the hotel business. Our hotels, as well as a wide range of businesses, rely on the Whois database to combat exploitation by malicious registrants who want to capitalize on our well-known trademarks, damaging our business and harming our customers. For years, individuals and entities have intentionally registered domain names that are identical or confusingly similar to those of well-known brands, such as Holiday Inn®, to lure Internet consumers and others to illegal, inappropriate, and deceptive websites under false pretenses. This practice of cybersquatting continues to evolve in complexity, sophistication and frequency, while the means to combat it remain relatively static. Activities such as phishing and typosquatting pose a danger to our customers and diminish the value of our brands. As a result, we are compelled to dedicate significant resources to pursuing trademark violations through various means, including the Uniform Domain Name Dispute Resolution Policy (UDRP).

The Study of Whois Privacy and Proxy Service Abuse confirms IHG's experience in dealing with malicious registrants that "a significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity." The Study further finds that "one way or another, those registering domain names to be used for criminal activity seldom provide valid contact information."

IHG has filed a number of UDRP complaints against registrants who used privacy or proxy services. In one UDRP proceeding this year, for example, IHG filed (and won) a UDRP complaint regarding the domain name <hotelindigoshanghai.com> (which contains IHG's trademark HOTEL INDIGO). The domain name was being used in connection with a website for a tour company that purportedly offered hotel reservations. *Six Continents Hotels, Inc. v. Domains By Proxy, LLC, DomainsByProxy.com / Peiyan Yao*, WIPO Case No. D2013-0660. See also *Six Continents Hotels Inc. v. Registrant [721393]: St Kitts Registry*, WIPO Case No. D2007-0758.

By utilizing privacy or proxy services to mask their identities, cybersquatters make it more difficult and time-consuming for IHG to successfully take advantage of the UDRP process given the challenge in identifying multiple domain names registered by a single cybersquatter and by the amendment typically required by UDRP service providers in complaints filed against privacy and proxy services.

As the Study points out, "there can be significant economies of scale in taking action to deal with many types of intellectual property infringement if it can be ascertained that a large number of relevant domains have been registered with essentially identical contact details...[T]he use of privacy or proxy services makes it very difficult for a brand owner to balance the costs against the benefits when considering proceedings to defend their rights." Further, the Study concludes that "there is clearly some incentive for registrants to hide their identities from casual inspection and to diversify their registrations."

These findings underscore that privacy and proxy services have become a widely used tool for registrants hoping to hide themselves from the public. IHG acknowledges that there may be legitimate reasons for lawful registrants to use a privacy or proxy service. Therefore, it is not our position to halt these services in their entirety; rather, we call on ICANN to develop effective enforcement mechanisms to assure that privacy and proxy administrators maintain accurate information of the registrants who contract their services and that, in the case of a legitimate dispute, there needs to be an appropriate, workable and timely process to obtain the underlying registrant's information.

This Study corroborates the need to move quickly to implement a Preliminary Recommendation included in the Initial Report on the Thick Whois Policy Development Process that "the provision of thick Whois services should become a requirement for all gTLD registries, both existing and future." Requiring all gTLD registries to provide thick Whois services would greatly improve IHG's ability to combat cybersquatting by creating a database that is central, universal and, hopefully, accurate. It would provide greater protections for consumers as well as brand and intellectual-property owners, and would help to ensure the continued stability of the Internet. Further, we believe that a requirement for uniformity in Whois output, such as that

contained in the proposed 2013 Registrar Accreditation Agreement, also is essential to provide consistency and assure that the information is easy to parse. We urge ICANN to finalize the language of the proposed 2013 Registrar Accreditation Agreement (RAA) to require registrars to provide uniform Whois output. While we agree that the transition of the current thin gTLD registries must be carefully prepared and implemented, we urge that the transition occur sooner, rather than later.

The Study provides objective evidence to support the urgent need for ICANN to initiate processes to oversee and regulate privacy and proxy service providers. This oversight must be standardized, and requirements for registrars to meet accreditation standards must be contractual. Such oversight will result in clear, consistent and enforceable requirements for the operation of privacy and proxy services that are consistent with national laws and that strike an appropriate balance between stakeholders with competing, but legitimate, interests.

Sincerely,

A handwritten signature in black ink that reads "Michael Menis". The signature is written in a cursive, slightly slanted style.

Michael Menis  
Senior Vice President, Digital & Voice Channels