From: Stacey King <stacey@ipwizard.com>
Date: October 25, 2007 9:32:49 AM EDT
To: <vint@google.com>
Subject: FW: Public Comment and Support for Motion 2

Dear Mr Cerf

I wanted to take this opportunity and separately forward to the ICANN Board my company's comments on the GNSO Council Motions on Whois, posted to the ICANN web site today.

We understand that many times such comments do not separately make their way to the Board and have been encouraged to send them to the Board as well to ensure the Board has been provided with a number of viewpoints on an issue.

I thank you for your time and would be happy to discuss with you or any of the other members of the Board my company's comments.

With best regards
Stacey King

Stacey King
Senior Internet Lawyer, IP
Richemont
15 Hill Street, London, W1J 5QT, England
Tel: +44 (0)20 7514 2764
Fax: +44 (0)20 7493 1018
Email: stacey@ipwizard.com

------ Forwarded Message
From: Stacey King <stacey@ipwizard.com>
Date: Thu, 25 Oct 2007 14:23:20 +0100
To: <whois-comments-2007@icann.org>
Conversation: Public Comment and Support for Motion 2
Subject: Public Comment and Support for Motion 2

To: Internet Corporation for Assigned Names and Numbers and GNSO Council

Re: Comment on Access to Whois Data

Richemont, one of the world's leading luxury goods groups, welcomes this opportunity to provide comments on the GNSO Council Motions, WHOIS Task Force Report, WHOIS Outcomes Working Group Report, and ICANN Staff Overview of Recent GNSO Activity Concerning WHOIS (the "Report").

It is Richemont's understanding that there are three motions released for public consideration and comment concerning WHOIS. The motions all provide for very different results:

1. support and implement the Operational Point of Contact (OPoC) proposal as a replacement for the WHOIS;

2. conduct a comprehensive study on the registration characteristics, uses and abuses of WHOIS data and take the results of this study into account before deciding any next steps in WHOIS policy development; or

3. phase out current WHOIS contractual obligations for registries, registrars and registrants over the next year.

Richemont strongly supports the second motion calling for a comprehensive study on the registration characteristics, uses and abuses of WHOIS data and take the results of this study into account before deciding any next steps in WHOIS policy development. Adoption of motions one and three would cause significant difficulties in the ability for brand owners and law enforcement

to police illegal activity and/or intellectual property violations on the Internet.

The fame of Richemont's brands makes it susceptible to a wide variety of online fraud schemes: from traditional cybersquatting to online counterfeiting rings. Consequently, Richemont takes an active role in protecting the value of its brand and its customers on the Internet. In order to do so, however, Richemont must be able to identify and contact the person(s) or entities that perpetrate such fraud. Whois records are key to discovering contact information in a timely manner. As a result, Richemont cannot support motions one and three as disabling access to WHOIS information directly affects Richemont's ability to timely conduct investigations and take appropriate actions.

Richemont views the data currently available in Whois records as critical to its ability to enforce its rights online. And Richemont is not alone in this assessment. Unfettered access to Whois records is needed by law enforcement, businesses, and individuals alike for the purpose of routing out counterfeiters, scammers and other nefarious online schemes. Such access is critical. In the 2004 Annual Enforcement Report of the U.K. Patent and Trademark Office the procedure taken to route out piracy of music discs is outlined. Law enforcement first visits a site, makes a test purchase, and then determines the physical location of the seller through Whois records and through tracing IP numbers. Indeed, in 2004 alone law enforcement officials, using this procedure, were able to conduct major raids in over 19 cities in the U.K. alone.

The U.K. is not the only law enforcement agency that uses Whois records. Law enforcement agencies from many jurisdictions have repeatedly documented the use of Whois records for investigation purposes -- often using such records as the first point of contact for identifying a web site owner and/or address. As with the U.K., law enforcement agencies in the United States also use Whois records as one of the first steps in conducting cybercrime investigations. In his 2003 testimony before the House Judiciary Subcommittee on Courts, the Internet and Intellectual Property, James E. Farnan, Deputy Assistant Director of the Cyber Division at the FBI stated that Cyber Division investigators use the Whois database almost every day to identify operators of questionable sites. He noted that investigators use the Whois database in investigations ranging from online fraud to computer intrusion cases and that the information from the Whois database is "often used to generate investigative leads and is the starting point for utilizing investigative techniques." Mr. Farnan also noted that the ability to use the publicly available Whois database was critical to investigations as it is "quicker to use Whois to obtain instant electronic access to data that could identify the perpetrator of a crime, as opposed to serving a subpoena or court order and waiting on a third party to deliver the same information." Speed is often of the essence in tracking down and stopping online crime.

The need to access these databases is similarly important for private businesses and individuals not only in the U.K., but around the world. Where law enforcement may have alternative mechanisms for tracking down the owners of fraudulent websites, private business and individuals do not. When a company finds a website selling counterfeit goods or misusing a trademark in the domain name, the Whois record is most often the primary means for determining the identity of the website operator. The same holds true for an individual who purchases an item from that site. Often the contact information found on the site itself may include only an e-mail address. The Whois records provide additional information that allow a business and/or consumer to contact the website owner, find out the ISP used by the website owner, and the name of the registry used to register the domain name. As with law enforcement, speed is often of the essence in these cases. Owners of fraudulent websites often act under numerous monikers and change ISPs regularly to make it hard to track them down. If a consumer had to contact a domain name registrar to make a complaint and then wait for the registrar to process the complaint and respond, the fraudulent site will often have already been moved making the consumer have to start the process

anew. We have experienced this on several occasions in connection with several registrars' current privacy controls that are supposedly limited to non-commercial sites, but are instead often used by suspect commercial sites.

For this reason, unfettered public access to Whois databases is crucial. Indeed, some countries have even started making public access to reliable and accurate contact information for each domain name registrant a part of its free trade agreements with other countries. For example, both the U.S.-Peru Trade Promotion Agreement, Article 16.4.2, and the U.S.-Morocco Free Trade Agreement, Article 15.4.2, require such public access to a reliable and accurate database of contact information. The United States also passed the Fraudulent Online Identity Sanctions Act which provides for increased damages in trademark cases where a registrant makes use of fraudulent, false Whois information.

Whois records are also used by UDRP panelists. In Thomas Cook Holdings Limited v. Matthew Dinham, WIPO D2000-0725, the panelist notes the following:

"The WHOIS records for the domain name club1830.com show the Respondent personally as the registrant with an email address mattd@leisuregroup.co.uk. This immediately implied to the Panelist that Mr. Dinham's business was likely to be connected with the leisure industry. A check at www.leisuregroup.co.uk <file://localhost/exchweb/bin/redir.asp> brought up the message "Welcome to Leisure Group -- Britain's number one for Sunbeds, Tanning Accelerators, Slimming Products, Sauna, Steam Rooms and all related accessories." A check of the WHOIS for leisuregroup.co.uk revealed that this domain name is also registered personally to Mr. Dinham. A further check for registrations in Mr. Dinham's name also revealed that, amongst other domains, the same Mr. Dinham is also the personal registrant of the domain name qualityflights.com -- the URL www.qualityflights.com <file://localhost/exchweb/bin/redir.asp> also resolves to a multilingual parking page as for www.club1830.com <http://www.club1830.com/> . It appears, therefore, that the Respondent, even if he is not presently in direct competition with the Complainant, has not been entirely candid about the nature of his business interests."

Again, if a consumer or a business had to make repeated requests to a registrar to obtain the information noted above, investigations would become incredibly lengthy in nature and the registrant would have the chance to transfer a domain name to another registrar or ISP.

Finally, there are entities that make fraudulent use of the Internet through registering numerous domain names and who have close relationships to registrars. Registrars may have policies that require them to inform their clients of queries into Whois information. In either case, owners of fraudulent sites would be given the opportunity to transfer domain names, websites, ISPs, etc. before a consumer, business, or law enforcement even has the registration information. This is not to say that the majority of registrars are suspect. However, it only takes one or two suspect registrars, known in the counterfeit or cybersquatting world, to create incredible difficulties to consumers and businesses alike.

We understand the problems and costs associated with registrars or registries ensuring that the data in Whois records is accurate and/or ensuring through follow-up investigations that those registrants who claim privacy rights based on a non-commercial site are indeed operating a non-commercial site. We ask the GNSO Council, however, to consider alternative scenarios that adoption of motions one and three may create whereby consumers and businesses are forced to sue registrars to obtain Whois information or claim a registrar is aiding online fraud, must name the registrar as the defendant in an action for lack of an alternative party or where registrars/oPOCs take too much time to respond, and/or where law enforcement is constantly serving subpoenas on registrars -- or even warrants to seize databases. In the meantime, more criminals are able to evade law enforcement. The cost to registrars and interested parties alike in this

situation would be incredible. Similarly, in certain situations registrars and oPOCs could be liable to domain name registrants for improperly releasing registrants' private information.

We believe access to the Whois database should not be limited in terms of public access. Motions one and three, as currently stated, would result in a haven for cybersquatters, online fraudsters, spammers, and scammers.

Respectfully submitted,
/Stacey King/

Stacey King
Senior Internet Lawyer, IP
Richemont
15 Hill Street, London, W1J 5QT, England