WHOIS subteam meeting with the ICANN compliance team

July 21, 2011

Attendees

Amy Stathos Deputy General Counsel

Maguy Serad - Senior Director of Contractual compliance

Stacy Burnette - Director, Contractual Compliance

Khalil Rasheed - Sr. Manager, Contractual Compliance

Denise Michele

Bill Smith

James Bladel

Susan Kawaguchi

The WRT subteam met with the ICANN compliance team in Marina Del Rey at their corporate office on July 21st.

Agenda

**AOC Whois Subcommittee ICANN Contractual Compliance Agenda Thursday 21 July 2011**

1. Staff Introductions and Overview
2. Key Compliance Activities Re: Whois
3. Whois Data Problem Report System
   1. System Demonstration
   2. Case Study
4. Whois Monitoring Tool (Port 43 Tool)
   1. Interface Demonstration
   2. Case Study
5. Whois Data Reminder Policy
   1. Questionnaire
   2. Key Findings
   3. Trends
6. Lunch 12:00 – 1:15 pm
7. AOC Subcommittee Members Substantive Discussion (By Request)
   1. Susan K. – Whois Misdirecting and Online Fraud
   2. James B. – GoDaddy’s Whois Inaccuracy Investigation Best Practices
   3. Other Issues ?
8. Feedback and Wrap-up

Whois Data Problem Report System

<http://wdprs.internic.net/>

“All accredited registrars have agreed with ICANN to obtain contact information from registrants, to provide it publicly by a Whois service, and to take reasonable steps to investigate and correct any reported inaccuracies in contact information for domain names registered through them.

Reports submitted through this system will be forwarded to the appropriate registrar for handling, and the progress of your report will be tracked. “

ICANN receives the report of inaccurate data but cannot act on it to correct the data, the registrar must take action by notifying the registrant of the alleged inaccuracy. The registrant has 15 days to respond and either correct the data or verify that the data is correct.

The registrar must respond affirmatively that they have notified the registrant but ICANN does not collect information on the change to the registration if any. ICANN also does not collect data on the number of domain names that are suspended due to inaccurate data.

ICANN recently improved their tool to track these reports and were able to show us data.

We discussed misuses of this system as there are many instances of erroneous reports. (Facebook frequently receives reports of inaccurate data in the WHOIS record when, in fact, it is accurate)

Suggestions

1. Track reports by user this would help to combat malicious use
2. Full disclosure by registrar of action taken (this may be more of a burden on the registrar than it would be worth)

**Whois Monitoring Tool (Port 43 Tool)**

3.3.1 At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy

Whois Access Audit Report (Port 43) http://www.icann.org/en/compliance/archive/whois-access-audit-report-port43-06apr11-en.pdf

Since Fall of 2010 ICANN automatically pings the IP address for each registrar four times a day to insure that Port 43 is accessible. Most registrars are in compliance. For those that are not, the compliance team will wait several days and if still not available then they will reach out to the registrar this allows for temporary technical failures. They have had to escalate with a few registrars and have issued two Notification of Breach for Port 43 failure.

They also routinely conduct a manual WHOIS query to insure the information is available.

**WHOIS Data Reminder Policy**

“At least annually, a registrar must present to the registrant the current Whois information, and remind the registrant that provision of false Whois information can be grounds for cancellation of their domain name registration. Registrants must review their Whois data, and make any corrections.”

**What the WDRP Notice Must Include:** Each WDRP notice must include a copy of the data elements listed in [RAA subsection 3.3.1](http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.3.1) as contained in the registrar's database for each registration, plus a statement reminding the registrant that under the terms of the registration agreement [the provision of false Whois information can be grounds for cancellation of a domain name registration](http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.7.7.2).

**How, and to Whom, the WDRP Notice May Be Presented:** The WDRP Notice can be presented via web, fax, postal mail, e-mail, or other appropriate means. It can be presented in one or more languages, including at least the language of the registration agreement. The Notice may be presented to the registrant either directly or through the administrative contact for each registration.

**Documentation Requirements:** Registrars [must maintain](http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.4) either copies of each WDRP Notice or an electronic database documenting the date and time, and the content, of each WDRP notice sent under this policy. Registrars shall [make these records available for inspection by ICANN](http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.4.3) in accordance with the usual terms of the Registrar Accreditation Agreement. ICANN will consider proper notification to have been given for a registration if the registrar can show that a WDRP Notice meeting the requirements stated above was given at any time in the year before each anniversary of the registration's creation date (for anniversary dates on or after the Compliance Date).

Dear Valued Customer,

This message is a reminder to help you keep the contact data associated with your domain registration up-to-date. Our records include the following information:

Domain: example.com  
Registrar Name: IANA\_RESERVED

Registrant:  
Name: Internet Assigned Numbers Authority (IANA)  
Address: 4676 Admiralty Way, Suite 330  
City: Marina del Rey  
State/Province: CA  
Country: US  
Postal Code: 92092

Administrative Contact:  
Name: Internet Assigned Numbers Authority (IANA)  
Address: 4676 Admiralty Way, Suite 330  
City: Marina del Rey  
State/Province: CA  
Country: US  
Postal Code: 92092  
Phone: 310-823-9358 begin\_of\_the\_skype\_highlighting              310-823-9358      end\_of\_the\_skype\_highlighting  
Fax: 310-823-8649  
Email: res-dom@iana.org

Technical Contact:  
Name: Internet Assigned Numbers Authority (IANA)  
Address: 4676 Admiralty Way, Suite 330  
City: Marina del Rey  
State/Province: CA  
Country: US  
Postal Code: 92092  
Phone: 310-823-9358 begin\_of\_the\_skype\_highlighting              310-823-9358      end\_of\_the\_skype\_highlighting  
Fax: 310-823-8649  
Email: res-dom@iana.org

Original Creation Date: 11/01/2001  
Expiration Date: 11/01/2001

Nameserver Information:  
Nameserver: a.iana-servers.net.  
Nameserver: b.iana-servers.net.  
Nameserver: c.iana-servers.net.

If any of the information above is inaccurate, you must correct it by visiting our website. (If your review indicates that all of the information above is accurate, you do not need to take any action.) Please remember that under the terms of your registration agreement, the provision of false Whois information can be grounds for cancellation of your domain name registration.

Thank you for your attention.

Best regards,  
Your ICANN-Accredited Registrar

The compliance team audits each registrar once a year by sending out a questionnaire asking a variety of questions including number of registrations, language, data that was updated.

In the last audit 5 registrars did not respond. In this case, the team will then contact each registrar and follow up to get information.

**WHOIS Misdirecting and Online Fraud**

Facebook continually finds domain names that are registered using Facebook, Inc. corporate information. Registrants do this so that if anyone checks the WHOIS record they would assume it is a legitimate registration and owned by Facebook, Inc. As the Domain Name Manager I am often fooled at first glance.

This registration has used correct information for the company the only two fields that are not accurate are the servers and email address.

Registrant:

Facebook Inc

1601 S. California Ave

California, California 94304

US

Domain name: FACEBOOK-MEMBERS.COM

Administrative Contact:

Members, Facebook hkhanzadeh@gmail.com

1601 S. California Ave

California, California 94304

US

+1.6505434800

Technical Contact:

Members, Facebook hkhanzadeh@gmail.com

1601 S. California Ave

California, California 94304

US

+1.6505434800

Registration Service Provider:

Hiberd Corp, info@hiberd.com

00982183804

Registrar of Record: TUCOWS, INC.

Record last updated on 17-Feb-2011.

Record expires on 17-Feb-2012.

Record created on 17-Feb-2011.

Registrar Domain Name Help Center:

http://tucowsdomains.com

Domain servers in listed order:

NS2.SYSTEMDNS.COM

NS3.SYSTEMDNS.COM

NS1.SYSTEMDNS.COM

This registration is using an email address that I know, as a Facebook employee, is not a working email address. Whatever the “real” registrant had intended to do with the registration he cannot control it since he does not have control of the admin contact email address. Definitely a throw away registration but potential for harm.

Registrant:

Facebook LLC

none

none, none 4119

NF

Domain name: LORDFRANCIS.COM

Administrative Contact:

Book, Face admin@facebook.com

none

none, none 4119

NF

4116353

Technical Contact:

Book, Face admin@facebook.com

none

none, none 4119

NF

4116353

Registration Service Provider:

SWsoft Inc., support@myplesk.com

This company may be contacted for domain support questions.

Registrar of Record: TUCOWS, INC.

Record last updated on 31-Jul-2011.

Record expires on 10-Jul-2012.

Record created on 10-Jul-2011.

Registrar Domain Name Help Center:

http://tucowsdomains.com

Domain servers in listed order:

NS3.AFRAID.ORG

NS2.AFRAID.ORG

NS1.AFRAID.ORG

NS4.AFRAID.ORG

Once again all information is correct and the email address would appear to be accurate but it isn’t. The servers are based on a .ir (Iran) domain registration.

Domain Name: GROUP-FACEBOOK.COM

Registrant:

Facebook, Inc.

Domain Administrator (FACEBOOK@FB.COM)

Palo Alto CA 94304 US

California

California,94304

US

Tel. +1.6505434800

Fax. +1.6505434800

Creation Date: 11-Mar-2011

Expiration Date: 11-Mar-2012

Domain servers in listed order:

ns1.youhosting.ir

ns2.youhosting.ir

Administrative Contact:

Facebook, Inc.

Domain Administrator (FACEBOOK@FB.COM)

Palo Alto CA 94304 US

California

California,94304

US

Tel. +1.6505434800

Fax. +1.6505434800

Technical Contact:

Facebook, Inc.

Domain Administrator (FACEBOOK@FB.COM)

Palo Alto CA 94304 US

California

California,94304

US

Tel. +1.6505434800

Fax. +1.6505434800

Billing Contact:

Facebook, Inc.

Domain Administrator (FACEBOOK@FB.COM)

Palo Alto CA 94304 US

California

California,94304

US

Tel. +1.6505434800

Fax. +1.6505434800

We walked through several similar registrations with the compliance team. (I reported or took control of some of the examples I used in July ) All of the above I can report as inaccurate or work with the registrar to gain control of the domain name.

It seems that there should be a way to circumvent a registration that is blatantly using fake information. It is a major concern that anyone can pose as a large company and the information in the WHOIS record in not validated.

ICANN staff seemed to have a lower threshold on inaccurate data than I had assumed.

**GoDaddy’s Whois Inaccuracy Investigation Best Practices**

James presented a document on best practice recommendations that GoDaddy staff drafted.

“In summary, we have undertaken an internal review & enhancement of our own practices in this area, and are exchanging some ideas with ICANN on improvements to their own WDPRS system, along with suggestions for other registrars in general.”

Recommendations

Bill Smith – Create a rating system so that it is easy to see what registrars are compliant but adjust scale for volume.

James – Standardize WHOIS output, control volume of WHOIS access to prevent mining

Susan – Compliance team should meet with registrants and explain how and what should be reported to them. Discussed hosting a meeting at FB with local businesses.