

COALITION FOR ONLINE ACCOUNTABILITY

WWW.ONLINEACCOUNTABILITY.NET

1818 N STREET N.W., 8TH FLOOR • WASHINGTON, D.C. 20036-2406 • TEL: (202) 355-7906 • FAX: (202) 355-7899 • E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

COMMENTS OF COALITION FOR ONLINE ACCOUNTABILITY

March 24, 2010

The Coalition for Online Accountability (COA) appreciates the opportunity to contribute to the development of the first Joint Strategic Plan called for under the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act). See 75 Fed. Reg. 8137 (Feb 23, 2010).

Introduction

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners. These are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. The Coalition's main goal is to preserve and enhance online transparency and accountability, by ensuring continued access to the information needed to carry out effective licensing and enforcement of intellectual property rights in the online environment. This includes access to accurate and reliable data on domain name registrants, as a key tool against online infringement of copyrights and trademarks, as well as to combat trademark infringement, cybersquatting, phishing, and other criminal or fraudulent behavior online.

Numerous submissions in response to this Federal Register notice, including some made or joined in by COA participants, stress the serious threat posed to the U.S. economy by rampant online infringement of copyrights and trademarks. COA believes that one focus of the Joint Strategic Plan should be to ensure that those who enforce the copyright and trademark laws online have the necessary access to information needed to perform this function. To advance this goal, U.S. policy should remain dedicated to preserving and enhancing a key tool that intellectual property right holders, and law enforcement, rely on every day to identify, track and pursue the parties responsible for this threat. That tool is Whois data. The U.S. government should continue its long-standing policies to keep this information publicly accessible, and to improve its reliability.

Access to Whois Data

Whois data includes contact information on the registrant of Internet domain names, as well as data on administrative and technical contacts, and leads for identifying the entity hosting

American Society of Composers
Authors & Publishers (ASCAP)

Entertainment Software Association (ESA)

Software & Information Industry Association (SIIA)

Broadcast Music Inc. (BMI)

Motion Picture Association of America (MPAA)

Time Warner Inc.

Recording Industry Association of America (RIAA)

The Walt Disney Company

Counsel: Steven J. Metalitz (met@msk.com)

the content on World Wide Web sites associated with the domain. It is made publicly available by domain name registrars – the entities that sell domain names to customers – and in many instances also by domain name registries – the “wholesalers” of domain names that maintain the authoritative database of registrations in a specific Top Level Domain (for instance, .com, .net, or .us).

Public access to Whois data is essential to the investigation and prompt resolution of instances of copyright piracy and trademark counterfeiting online. The investigation of virtually every such case involves the use of Whois data. For example, when an investigator seeks to determine who is responsible for a website where infringing activity is taking place, a review of the Whois data for the domain name which resolves to that site is usually the first step. Once the responsible party has been identified, the copyright owner or its agent is in a position to request that the party obtain a license or cease the infringing activity, or, where appropriate, to begin enforcement action. But Whois data’s valuable uses are by no means limited to the sphere of intellectual property protection. Access to Whois data is critical to dealing with instances of phishing, distribution of malware, network attacks, and online frauds of all kinds. This data is essential to law enforcement, of course, but also to private parties such as copyright and trademark owners, whose independent enforcement of their rights allows law enforcement to conserve scarce resources. Indeed, virtually every Internet user benefits: Whois provides greater transparency, so that end users know more about the parties with whom they – or their children – are interacting online. In this way, publicly accessible Whois promotes the healthy growth of e-commerce, including but not limited to e-commerce in works protected by copyright.

The U.S. government can preserve public access to Whois in three main ways, depending on the type of domain name registration involved:

- With regard to generic Top Level Domains (gTLDs), such as .com, .net, or .info, public accessibility of Whois depends on the terms of contracts between the registrars (and registries) and the Internet Corporation for Assigned Names and Numbers (ICANN). The U.S. government participates in ICANN primarily through the ICANN Governmental Advisory Committee.
- With regard to country code Top Level Domains (ccTLDs), such as .uk, .fr, and .de, ICANN plays almost no role on Whois. Here, the U.S. government’s interest in publicly accessible Whois can be expressed through a number of bilateral channels. For instance, the U.S. has entered into free trade agreements (FTAs) with several countries that set baseline standards that our trading partners pledge to maintain in the ccTLDs allocated to each country. These standards include providing public access to reliable and accurate contact information on domain name registrants.¹

¹ See, e.g., Australia FTA, Art. 17.3; Chile FTA, Art. 17.3; Peru FTA, Art. 16.4; Singapore FTA, Art. 16.3. All these texts are accessible via <http://www.ustr.gov/trade-agreements/free-trade-agreements>. These FTA provisions also require trading partners to employ dispute resolution systems in their ccTLDs based on the Uniform Dispute Resolution Policy (UDRP) mandated by ICANN for use in all gTLDs. See Uniform Domain Name Dispute

(...continued)

- With regard to our own national ccTLD, .us, Whois policy is set by the National Telecommunication and Information Administration (NTIA) of the U.S. Department of Commerce.

The U.S. government has consistently used all these channels to advocate for maintaining the unfettered public access to Whois that has been the norm since the earliest days of the Internet. For example, in the Joint Project Agreement between ICANN and the Department of Commerce that expired last September, ICANN explicitly committed to maintaining the current policy requiring publication of Whois data. NTIA has set a similar policy for .us.

Going forward, it is crucial that the U.S. government reaffirm its stance in favor of publicly accessible Whois. Under the Affirmation of Commitments that now embodies the U.S. government's relationship with ICANN, a review of Whois policy is scheduled to be launched later this year.² The U.S. government should participate actively in that review to ensure that this critical enforcement tool remains available in the gTLD environment. With respect to ccTLDs, the U.S. should insist on provisions regarding publicly accessible Whois in all future Free Trade Agreements.

Accuracy and Reliability of Whois Data

Beyond the question of Whois access, action is clearly needed to make Whois data more reliable and to reduce the current extremely high level of inaccuracy and outright fraud in Whois data.³ While even inaccurate Whois data often has investigative value, greater efforts to ensure that Whois data is accurate, complete and current could pay significant dividends in faster, more efficient enforcement against online piracy and counterfeiting.

ICANN currently is preparing to open the doors for applications for hundreds or perhaps even thousands of new gTLDs. This is the third new gTLD round that ICANN has held since its inception, but it will be by far the biggest, and is expected to set the ground rules for additional rounds into the future. Working through the GAC and in other fora, the U.S. government should

(...continued)

Resolution Policy, <http://www.icann.org/en/dndr/udrp/policy.htm>. The UDRP has been an important tool for trademark owners in combating abuse of their marks online through cybersquatting.

² See <http://www.icann.org/en/documents/affirmation-of-commitments-30sep09-en.htm>, at paragraph 9.3.1.

³ ICANN recently released a years-long study on the accuracy of Whois data that confirmed previous smaller studies, including one by the Government Accountability Office in 2005, showing very high levels of false data. See United States Government Accountability Office, Report to the Subcommittee on Courts, the Internet, and Intellectual Property, House of Representatives, Internet Management: Prevalence of False Contact Information for Registered Domain Names (2005), available at <http://www.gao.gov/new.items/d06165.pdf> (“In total, GAO estimates that 3.89 million domain names (8.65 percent) had at least one instance of patently false or incomplete data in the required Whois contact information fields.”); see also National Opinion Research Center, University of Chicago, Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information (2010), available at <http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf>.

support ground rules that set a greater emphasis on the need for the new gTLD registries (directly, or through the registrars authorized to take registrations) to verify contact data submitted by registrants, and to cancel registrations that are supported by intentionally falsified contact data.

The U.S. government should also monitor closely the negotiation of new amendments to the standard Registrar Accreditation Agreement that all domain name registrars must sign with ICANN in order to be authorized to sell registrations in any gTLD. This amendment process will address a number of issues having to do with reliability of Whois data.⁴

IP Address Whois

The label “Whois” also refers to information about the allocation of blocks of Internet Protocol (IP) addresses, which are the numeric addresses for all resources connected to the Internet. Access to this information is extremely important for enforcement against copyright piracy, trademark infringement, and other forms of misconduct carried out online. When such misconduct is associated with a particular IP address, Whois enables the investigator to identify the Internet service provider or other entity to which the IP address was initially assigned, and also to learn of sub-allocations to other providers, though rarely, if ever, to the end-user.⁵ Accessibility and reliability of IP address Whois data, including ensuring that all sub-allocations are entered into the database and kept up to date, are also critical issues for attention from the U.S. government. Policies on these questions are generally set by the five Regional Internet Registries (RIRs) that receive initial allocations of IP addresses from the Internet Assigned Numbers Authority, operated by ICANN under contract to the U.S. Department of Commerce. Under the Joint Strategic Plan, appropriate U.S. government agencies should remain engaged with the RIRs on these issues.

The Broader Issues

Finally, as noted at the beginning of this submission, questions regarding access to Whois data are a subset of a broader range of issues related to ensuring that those who enforce the copyright and trademark laws have the access to information needed to perform this function. While of course this category includes law enforcement agencies, the vast majority of intellectual property enforcement activities are, and in the United States always have been, carried out by private sector actors, including for example COA participants. Nor are law enforcement

⁴ COA commends the recent submission, by law enforcement representatives from the U.S. and six other countries, of suggestions for topics to be addressed in amendments to this standard agreement, including several suggestions aimed at improving the accessibility and reliability of Whois data. The ICANN Governmental Advisory Committee recently urged ICANN to give these proposals serious consideration. See http://gac.icann.org/system/files/Nairobi_Communique_0.pdf, item VI.

⁵ Since IP Whois address information by itself cannot identify any end-user, other than in exceptional cases, public access to such data has little if any impact on privacy or free expression concerns.

agencies anywhere in the world in the position to devote the resources and expertise needed to be the sole or even the primary mechanism for dealing with the piracy and counterfeiting that has become so pervasive in the online environment. Private sector access is needed, and this access is often in jeopardy, especially outside the United States, because of restrictions or barriers imposed on the basis of other laws, notably those for protecting individual privacy (or data protection, in European parlance).⁶ U.S. enforcement policy, as reflected in the Joint Strategic Plan, should include a focus on ensuring that this access is available for the purpose of enforcement of intellectual property laws by the private sector, with due consideration to reasonable concerns for the protection of individual privacy. Such access also seems fully compatible with the purpose for which Whois data has always been collected and made available to the public: primarily for the purpose of enabling contact with the operators of online resources to which domain names resolve (with respect to domain name Whois) or with the network operators to which an IP address has been allocated or sub-allocated (in the case of IP Address Whois). This is essentially the same use to which right holders put this data today.

Thank you for considering the views of COA. Please do not hesitate to contact the undersigned if further information is needed.

Respectfully submitted,

Steven J. Metalitz, counsel to COA

Mitchell Silberberg & Knupp LLP | 1818 N Street, N.W., 8th Floor, Washington, D.C. 20036 USA | tel: (+1) 202 355-7902 | fax: (+1) 202 355-7899 | met@msk.com

⁶ COA expressed its concerns on this issue in some detail in a public consultation held by the Article 29 Working Party consisting of data protection commissioners from European Union Member States. See Submission of COA, Public Consultation On Working Document No. 104, http://ec.europa.eu/justice_home/fsj/privacy/docs/intellectual_property_rights/coa_en.pdf.