

**Software & Information
Industry Association**

1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095



Prepared Statement of

**Mark Bohannon
General Counsel & Senior Vice President**

Software & Information Industry Association (SIIA)

**“ICANN and the Whois Database:
Providing Access to Protect Consumers from Phishing”**

**Before the
Subcommittee on Financial Institutions
And Consumer Credit**

U.S. House of Representatives

July 18, 2006

Tel: +1.202.289.7442

Fax: +1.202.289.7097

www.siiia.net

Mr. Chairman, members of the Subcommittee, I appreciate this opportunity to appear before you today and testify on ICANN and the Whois Database, an important tool for protecting consumers and promoting confidence in doing business online.

As the principal trade association of the software and digital information industry,¹ the Software & Information Industry Association (SIIA) has been engaged in the issue of Whois policy for several years, through its active participation in the Coalition for Online Accountability (COA), which consists of many leaders in the copyright industry.² COA's goal is to enhance and strengthen online transparency and accountability. It works to ensure that domain name and IP address in the Whois databases³ remain publicly accessible, accurate, and reliable. In my capacity as General Counsel & SVP Public Policy for SIIA, I actively participate in COA, serve on the Intellectual Property Constituency of ICANN and have seen first hand how the Whois database is a key tool to combat online copyright and trademark infringement, cybersquatting, phishing, and other fraudulent or criminal acts online, including the pernicious effects of spyware.

¹ The more than 750 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

² Formerly known as the Copyright Coalition on Domain Names, the Coalition for Online Accountability (COA) includes the American Society of Composers, Authors and Publishers (ASCAP); the Business Software Alliance (BSA); Broadcast Music, Inc. (BMI); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software & Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company.

³ "Whois" refers to the database of information identifying registrants of domain names. In the generic Top Level Domains (e.g., .com/net/org), this includes data on administrative and technical contacts for the registrants as well.

Whois data has been accessible to the public since the inception of the domain name system. Since 1999, Whois policies for the generic Top Level Domains (gTLDs) have been set by the Internet Corporation for Assigned Names and Numbers (ICANN). In contracts with the operators of the gTLD registries, and with every domain name registrar, ICANN requires that:

1. Domain name registrants must provide full and accurate contact data and keep it current; and
2. This contact data must be accessible to the public in real-time, without charge, via the Web, and without substantial restrictions on use.

The Importance of an Accurate, Complete and Accessible Whois

As you are well aware, Mr. Chairman, copyright owners battle an epidemic of online piracy. Whois is a key tool for investigating these cases and identifying the parties responsible. Every pirate site has an address on the Internet; and through Whois and similar databases, virtually every Internet address can be linked to contact information about the party that registered the domain name corresponding to the site; about the party that hosts the site; or about the party that provides connectivity to it. No online piracy case can be resolved through the use of Whois *alone*; but nearly every online piracy investigation involves the use of Whois data at some point.

Trademark owners use Whois in a similar way to combat cybersquatting, the promotion of counterfeit products online, and a wide range of other online infringement problems. They also depend on accurate and accessible Whois for a number of other critical business purposes, such as trademark portfolio management, conducting due diligence on corporate acquisitions, and identifying company assets in insolvencies/bankruptcies.

Enforcing intellectual property rights is only one of the beneficial uses of Whois data. Others include:

- **Consumer protection**: As the FTC has already explained, they rely upon accessible and accurate Whois data to track down online scam artists, particularly in cross-border fraud cases that are increasingly at the forefront of consumer protection agencies agendas around the world. Leading consumer protection and privacy advocacy groups have relied on Whois to track down deceptive claims for use of trusted seal marks,⁴ and the Center for Democracy and Technology has found the Whois Database a critical tool in bringing their high profile complaints

⁴ Statement of Lori Fena, Chairman of the Board of Truste, Before the Subcommittee on Courts, The Internet and Intellectual Property House Judiciary Committee, July 12, 2001, found at: http://judiciary.house.gov/Legacy/fena_071201.htm. (“... the WHOIS database has been and continues to be instrumental in enabling TRUSTe to have fraudulent TRUSTe privacy seals removed from Web sites. Consumers also use the WHOIS database as a resource for determining where a company is located and how to contact them. Accurate contact information from a reliable source provides consumers with the assurance that the company can be held accountable and gives them the means for pursuing recourse. In order for this database to be efficient and effective for both consumers and businesses, the public information needs to be accurate and accessible.”)

against spyware distributors and educating consumers on the pernicious effects of harmful downloads.⁵

- **Law enforcement**: The role Whois data plays in law enforcement investigations is well documented. Indeed, at an ICANN meeting last year in Luxembourg, law enforcement officials from several countries – including Australia, U.K., Spain, Japan and Malawi, as well as from Interpol – provided case studies of their use of Whois data to solve complex cybercrimes and enforce other criminal laws. At SIIA, we work with law enforcement in the development of criminal copyright infringement and similar cases, and we know first-hand that public access to this data is critical to facilitate the gathering of evidence that can assist law enforcement in prosecuting cases of crimes carried out online.
- **Network security**: The applications of Whois data in this arena deserve more attention than they have received. When a virus is detected, a denial of service attack unfolds, or another threat to the security of networked computing resources is identified, the response often requires instantaneous access to Whois data. ICANN’s own expert Security and Stability Advisory Committee concluded that “Whois data is important for the security and stability of the Internet” and that “the accuracy of Whois data used to provide contact information for the party responsible for an Internet resource must be improved.”

⁵ See, e.g., In the matter of Mp3DownloadCity.com and MyMusicInc.com, (<http://cdt.org/copyright/20050308complaint.pdf>); In the Matter of MailWiper, Inc., and Seismic Entertainment >Productions, Inc., (<http://cdt.org/privacy/20040210cdt.pdf>); In the Matter of Integrated Search Technologies, et al (<http://cdt.org/privacy/20051103istcomplaint.pdf>); In the Matter of 180solutions (<http://cdt.org/privacy/20060123180complaint.pdf>); In the Matter of 180solutions, Inc. and CJB.NET, (<http://cdt.org/privacy/20060123cjb.pdf>); “Following the Money: How Advertising Dollars Encourage Nuisance and Harmful Adware and What Can be Done to Reverse the Trend, (<http://www.cdt.org/privacy/20060320adware.pdf>).

In practice, several of these well-established and vital uses of Whois data often overlap. The continuing plague of cases of “phishing” or “corporate identity fraud,” as well as other types of online financial scams, are good examples, and as you will be hearing today from the financial services sector, access to Whois data is critical for resolving these cases as quickly as possible.

In the simplest example of a “phishing” attack – there are many variations of course -- hackers set up “cloned sites” on the Internet that skillfully imitate the look and feel of the sites of major financial institutions, online service providers, or E-commerce companies. These fraud artists then send mass e-mails to depositors, subscribers, or other customers of the legitimate companies, directing them to the cloned site where they are asked to provide social security numbers, PIN numbers, credit card numbers or other sensitive personal information, purportedly to “verify,” “update,” or “renew” their accounts. As the former chairman of the FTC has observed, “Phishing is a two time scam. Phishers first steal a company’s identity and then use it to victimize consumers by stealing their credit identities.”

Phishing is thus not only of concern to law enforcement agencies, consumer protection groups, intellectual property owners, and network security specialists: it also threatens the personal privacy of every consumer who is active online. Ready access to accurate Whois data can play a critical role in determining who is engaged in this scam and in bringing them to justice. Indeed, if the quality of Whois data were considerably more accurate than it is today, then it would be that much more difficult for this type of destructive fraud to be carried out.

Whois data has other important uses. It helps parents know who stands behind sites their children visit online; it helps consumers determine who they are dealing with when they shop online; and it plays a role in ferreting out the source of e-mail spam. In short, all Internet users need Whois to provide essential transparency and accountability on the Internet. We all have a stake in preserving and enhancing real-time access to this database, and in improving its quality and reliability.

Recent Moves to Restrict Access to Whois

Against this backdrop, SIIA and other copyright and trademark interests were seriously concerned when the body charged with developing policies for the “generic Top Level Domains,” notably .com, .net and .org – the GNSO Council at ICANN – adopted a resolution defining the “purpose of Whois” in the most narrow, technical terms.

Specifically, the Council voted that the *only* purpose of Whois should be to “resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver.” This formulation covers only a very small proportion of the current, critical uses of publicly accessible Whois data. Virtually all the ways that Whois is now used to protect intellectual property rights, investigate crimes, fight fraud and phishing, and protect privacy online would fall outside the scope of this definition of the purpose of Whois.⁶

⁶ This is not an abstract philosophical question. Whatever ICANN decides about the purpose of Whois will have legal consequences. The current, long-standing system of unfettered public access to Whois data is enforced through contracts between ICANN and the domain name registries and registrars that it has accredited. Any newly announced “purpose of Whois” will almost certainly lead ICANN to modify its

The results of any such move could be devastating to businesses, consumers, and everyone who uses the Internet to shop, work or play. Most of the current public and business uses of Whois would become impossible, or at least much more difficult and costly to carry out. Broad public access to Whois, and a rich Whois data set with information on registrants and administrative contacts, generally isn't needed to resolve narrow technical issues. If the "purpose of Whois" is defined narrowly, most of the data now in Whois would be cut off from public access.

This dismaying prospect has galvanized concerns in many sectors about ICANN's stewardship of the Whois system. Even before the GNSO Council vote was taken, over 50 organizations/coalitions/corporations/individuals filed comments against the narrow formulation of the "purpose of Whois." These submissions came from 12 countries, and were made on behalf of a number of major Internet-oriented corporations. The American Red Cross also expressed concerns about the impact on its ability to shut down fraudulent fundraising sites, such as those that sprang up within hours after Hurricane Katrina hit the Gulf Coast last year.

Once the GNSO Council voted for the narrow formulation, concerns within the business community became even more widespread. I would be pleased to submit for the record a number of letters sent to the ICANN Board from representatives of sectors such as financial services, hotel and lodging, and trademark and anti-counterfeiting groups, all opposing the narrow formulation of the purpose of Whois, and spelling out its potential

contractual policies on Whois to conform to that "purpose." As a result, registrars and registries would no longer be required to make available any data about domain name registrants that was not essential to carry out the narrowly defined "purpose."

adverse impact on transparency and accountability online.

Finally, Mr. Chairman, your letter to Commerce Secretary Gutierrez has provided added impetus and urgency to the development of a strong U.S. government position on the issue of Whois policy within ICANN. We applaud the position that was presented at the ICANN meeting last month in Marrakech, Morocco, both by the US delegation to ICANN's Governmental Advisory Committee, and by FTC Commissioner Leibowitz. Significantly, that message was reinforced by several other governments within the GAC, as well as in a presentation to the GAC by the director of OPTA, the government agency in the Netherlands with consumer protection authority online, as well as by a representative of the Japanese Ministry of Information and Communications.

Is ICANN listening? We hope so. At the Marrakech meeting, the Whois issue was discussed in a number of fora. There was considerable backing away from the concept that the only purpose of making registrant contact data publicly available is to resolve technical problems – the fundamental underpinning of the narrow formulation of Whois adopted by the GNSO Council. And the task force within ICANN that is working on developing Whois policy set an ambitious timetable for coming up with recommendations before the end of this year so that they can be discussed at the next ICANN meeting, scheduled for early December in Brazil.

The Accuracy and Reliability of Whois Databases Must Improve

Preserving public access to Whois is critical; but equally essential is to drastically improve the accuracy and reliability of Whois data. The problem has been amply documented, most recently in a study released last December by the Government Accountability Office.⁷ Overall, GAO estimated that the Whois data on over 5 million domain names in .com, .net and .org is either obviously false, incomplete, or simply could not be found. This high level of inaccuracy significantly undermines the value of Whois. Certainly wrongdoers know that they can provide obviously phony Whois data and thus impede the effectiveness of Whois as a tool for maintaining accountability on the Internet.

The GAO study also clearly shows that the system ICANN has put in place to address this problem – the Whois Data Problem Reporting System (WDPRS) – simply does not work. GAO investigators submitted complaints about blatantly false data to the WDPRS, but after more than a month, the contact information had been corrected in only one-quarter of the cases. At least half the time, the phony data remained unchanged, and the domain name remained as active and accessible as before the complaint was made.

This hearing comes at a critical juncture in the relationship between the U.S. government and ICANN. ICANN carries out its activities under the authority of a Memorandum of Understanding (MOU) between it and the Department of Commerce.

⁷ “Internet Management: Prevalence of False Contact Information for Registered Domain Names” (GAO 06-165).

The current MOU expires on September 30. So the next few weeks and months are an opportune time to reflect on the job ICANN has done with respect to its stewardship of Whois, and to consider how, in the ongoing relationship between ICANN and the US government, we can encourage it to do better.

In the last renewal of the MOU, in 2003, ICANN pledged to take steps to improve the accuracy of Whois data. It also promised to put into place an enhanced system for ensuring that domain name registrars and registries live up to their contractual obligations to ICANN – including, though of course not limited to, their obligations to make Whois data publicly accessible and to deal with complaints about inaccurate data.

We understand that ICANN believes that it has fulfilled these pledges under the MOU. Candidly, we do not agree with this assessment. Although ICANN has taken some steps to improve the system for receiving and processing complaints about inaccurate Whois data, ICANN's own reports show that that system does not work as it was designed to do. More importantly, ICANN has consistently shied away from taking on the more difficult task of requiring registrars and registries to take some proactive steps – any proactive steps – to verify that the information they are collecting from domain name registrants for inclusion and public display via Whois is accurate and reliable. Finally, ICANN's contract compliance program exists on paper – or on the electrons of its website -- but there is very little evidence that it functions in practice or that any meaningful action has been taken against registrars or registries for non-compliance.

Conclusion

Beyond assessing ICANN's performance on the tasks it signed up for under the last MOU, the recent developments regarding the "purpose of Whois" make it timely to consider how best to ensure that ICANN does not set off down the path that would lead to a reversal or substantial erosion of the long-standing policy of making domain name registrant contact data accessible to the public in real-time, without charge, via the Web, and without substantial restrictions on use. That policy is in our national interest, in the interests of consumers and businesses worldwide, and in the interest of promoting the healthy growth of the Internet as a safe place to work, play and do business. We believe that this perspective must be appropriately reflected in the terms under which ICANN continues to carry out its extraordinarily critical task of managing the domain name system.

Thank you again, for convening this hearing. I would be glad to take any questions from the Subcommittee.