

INTERNET DOMAIN NAME FRAUD—THE U.S. GOVERNMENT'S ROLE IN ENSURING PUBLIC ACCESS TO ACCURATE WHOIS DATA

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 4, 2003

Serial No. 50

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

U.S. GOVERNMENT PRINTING OFFICE

89-199 PDF

WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
STEVE CHABOT, Ohio	MELVIN L. WATT, North Carolina
WILLIAM L. JENKINS, Tennessee	ZOE LOFGREN, California
CHRIS CANNON, Utah	SHEILA JACKSON LEE, Texas
SPENCER BACHUS, Alabama	MAXINE WATERS, California
JOHN N. HOSTETTLER, Indiana	MARTIN T. MEEHAN, Massachusetts
MARK GREEN, Wisconsin	WILLIAM D. DELAHUNT, Massachusetts
RIC KELLER, Florida	ROBERT WEXLER, Florida
MELISSA A. HART, Pennsylvania	TAMMY BALDWIN, Wisconsin
JEFF FLAKE, Arizona	ANTHONY D. WEINER, New York
MIKE PENCE, Indiana	ADAM B. SCHIFF, California
J. RANDY FORBES, Virginia	LINDA T. SANCHEZ, California
STEVE KING, Iowa	
JOHN R. CARTER, Texas	
TOM FEENEY, Florida	
MARSHA BLACKBURN, Tennessee	

PHILIP G. KIKO, *Chief of Staff-General Counsel*

PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

LAMAR SMITH, Texas, *Chairman*

HENRY J. HYDE, Illinois	HOWARD L. BERMAN, California
ELTON GALLEGLY, California	JOHN CONYERS, JR., Michigan
BOB GOODLATTE, Virginia	RICK BOUCHER, Virginia
WILLIAM L. JENKINS, Tennessee	ZOE LOFGREN, California
SPENCER BACHUS, Alabama	MAXINE WATERS, California
MARK GREEN, Wisconsin	MARTIN T. MEEHAN, Massachusetts
RIC KELLER, Florida	WILLIAM D. DELAHUNT, Massachusetts
MELISSA A. HART, Pennsylvania	ROBERT WEXLER, Florida
MIKE PENCE, Indiana	TAMMY BALDWIN, Wisconsin
J. RANDY FORBES, Virginia	ANTHONY D. WEINER, New York
JOHN R. CARTER, Texas	

BLAINE MERRITT, *Chief Counsel*

DEBRA ROSE, *Counsel*

DAVID WHITNEY, *Counsel*

MELISSA L. McDONALD, *Full Committee Counsel*

ALEC FRENCH, *Minority Counsel*

CONTENTS

SEPTEMBER 4, 2003

OPENING STATEMENT

	Page
The Honorable Lamar Smith, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Courts, the Internet, and Intellectual Property	1
The Honorable Howard L. Berman, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Courts, the Internet, and Intellectual Property	10

WITNESSES

Mr. Steven J. Metalitz, Partner, Smith and Metalitz, LLP, and Counsel, Copyright Coalition on Domain Names	
Oral Testimony	12
Prepared Statement	14
Mr. Benjamin Edelman, Fellow, Berkman Center for Internet and Society, Harvard Law School	
Oral Testimony	20
Prepared Statement	22
Mr. James E. Farnan, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation	
Oral Testimony	47
Prepared Statement	48
Mr. Theodore W. Kassinger, General Counsel, U.S. Department of Commerce	
Oral Testimony	50
Prepared Statement	51

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Letter to Secretary Donald Evans, U.S. Department of Commerce, from the Subcommittee	3
Letter from Theodore W. Kassinger, General Counsel, U.S. Department of Commerce, on behalf of Secretary Evans, to the Subcommittee	7
Letter from Margie Milam, General Counsel, eMarkmonitor, Inc. to the Subcommittee	66
Prepared Statement of the International Trademark Association	70

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Department of Commerce Statement regarding Extension of Memorandum of Understanding with the Internet Corporation for Assigned Names and Numbers	79
Prepared Statement of the Honorable Robert Wexler, a Representative in Congress From the State of Florida	89
Letter from Alan Davidson, Center for Democracy and Technology, to the Subcommittee	90
Letter from Brian Cute, Director of Policy, Network Solutions, Inc.; Elana Broitman, Director of Policy, Register.com; Tom D'Alleva, Vice President, Bulk Register; and Paul Stahura, President, eNom, to the Subcommittee	92

IV

	Page
Letter from Michael D. Maher, Chairman of the Board, Public Interest Registry, to the Subcommittee	95

INTERNET DOMAIN NAME FRAUD—THE U.S. GOVERNMENT'S ROLE IN ENSURING PUBLIC ACCESS TO ACCURATE WHOIS DATA

THURSDAY, SEPTEMBER 4, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:02 p.m., in Room 2141, Rayburn House Office Building, Hon. Lamar Smith (Chair of the Subcommittee) presiding.

Mr. SMITH. The Subcommittee on Courts, the Internet, and Intellectual Property will come to order. Today's hearing is on "Internet Domain Name Fraud—The U.S. Government's Role in Ensuring Access to Accurate Whois Data." I am going to recognize myself for an opening statement, then the Ranking Member, and then we will proceed to hear from our witnesses.

The August infection of more than 7,000 computers with a variant of the blaster worm serves as a graphic reminder of the dangers that persist for Internet users. As devastating as this attack was, the damage it caused pales in comparison to the nearly 63,000 viruses that have been released on the Internet, which have caused \$65 billion worth of damages. Yet only one person in the U.S. has received a prison sentence in connection with these crimes. The FBI's blaster investigation was assisted by the suspect's provision of truthful information to the Whois database upon registering his website, but this result is the exception rather than the rule.

Consumers, business owners, intellectual property holders, parents, and law enforcement officials understand that these attacks impose real and substantial costs on each of them and they have called out for tougher enforcement.

Copyright owners use Whois to identify pirated sites—excuse me, pirate sites that operate on the Internet. Trademark owners use Whois to resolve cyber squatting disputes, learn the contact details for owners of websites offering counterfeit products or otherwise infringing on intellectual property. And law enforcement officers use Whois as the first step in most web-based child pornography and exploitation cases.

The enforcement of contracts that already exist between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers, ICANN, and its registrars in the top-level domains, such as .com, .net, and .org, and the registrants who oper-

ate websites could do much to clean up the World Web. The task of concealing one's identity is made considerably easier when registrars refuse to take reasonable steps, as their contracts require, to ensure that website registrants accurately report their identity and contact information to the Whois database.

Since 1999, all accredited registrars have been required to provide access to the full database of registered domain names. Despite the demonstrated need and obligation of the Department of Commerce, ICANN, and the registrars to provide access to Whois data, there is an astonishing lack of enforcement of these contractual terms. In ICANN's history, not one registrar has had their accreditation revoked for failure to honor their Whois commitments. This is inexcusable.

Since the issuance of a Presidential directive in 1997, the responsibility for overseeing the Domain Name System (DNS) and managing the transition to private sector control of the technical functions of the Internet has resided with the National Telecommunications and Information Administration, an agency within the United States Department of Commerce. Pursuant to the directive, NTIA entered into a contract with the newly-formed Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. Since creation, ICANN's legitimacy and its activities have been the subject of constant controversy.

The Commerce Department's relationship with ICANN is governed by three major agreements: One, a Memorandum of Understanding (MOU) for a joint domain name system; two, a cooperative research and development agreement; and three, a sole-source contract to perform certain technical functions relating to the coordination of the DNS. In spite of a nearly 5-year-long relationship with ICANN, there is a growing awareness that Commerce has failed to exert its authority to ensure that the public domain name registrant databases known as Whois contain accurate information. Agreements that are not enforced undermine the very authority, stability, and sustainability that Commerce purports to want to ensure for ICANN.

With the current MOU due to expire September 30, Mr. Berman and I wrote Secretary Evans on August 8 requesting that, among other things, any succeeding MOU be limited to 1 year, preserve public access to online systems like Whois, and take steps to improve the integrity of registrant contact information. Without objection, that letter will be made a part of the record.

[The letter to Secretary Evans follows:]

August 8, 2003

The Honorable Donald Evans
Secretary
U.S. Department of Commerce
Washington, D.C. 20230

Dear Mr. Secretary:

As Chairman and Ranking Member of the Subcommittee on Courts, the Internet, and Intellectual Property, we are interested in developments that affect the operation of the Internet's Domain Name System (DNS) and the public domain name registrant database known as "Whois."

It is critical that the Department of Commerce exercise sustained vigilance over the Internet Corporation for Assigned Names and Numbers' (ICANN) and its role in implementing policies and decisions that affect DNS users.

With the current Memorandum of Understanding (MOU) between ICANN and the Department due to expire on September 30, we write to express our support for the inclusion of strong intellectual property enforcement provisions in any successive MOU. Additionally, to achieve maximum transparency and accountability, we urge the Department to limit any extension of the MOU to a one-year period.

In the transition to private management of the Internet, it is vitally important to (1) preserve public access to online systems, like Whois, which display contact information of owners of Internet addresses; and (2) improve the integrity of the contact information that is provided.

Law enforcement officials have said that continued access to accurate Whois data is necessary to identify and apprehend criminals, including child pornographers, those who commit fraud or piracy on the Internet, and individuals or groups that might threaten network security. Intellectual property owners and individual consumers rely on the

accuracy and public accessibility of Whois information to protect their rights and to pursue civil claims. Trademark and copyright owners, in particular, require accurate and accessible Whois data to resolve domain name disputes and investigate intellectual property violations such as piracy and counterfeiting.

The importance of providing Whois access is clear. ICANN's obligation to ensure such access is also clear. Since 1999, all accredited registrars have been required to provide public access to the full database of registered domain names. Explicit provisions of ICANN's Registrar Accreditation Agreement (RAA) require registrars to:

- inform registrants of their obligation to provide "accurate and reliable contact details and promptly correct and update" such information;
- obtain the consent of registrants to the specified use of their contact information;
- take steps to ensure that Whois data provided by registrants is accurate, complete, and current;
- respond to reports of false contact data;
- make specified Whois data publicly available online, in real time, and without charge; and
- provide "bulk Whois" data to third-party providers under stated terms and conditions.

Despite the demonstrated need and obligation for registrars to provide reasonable access to accurate Whois data, there is growing evidence that ICANN has failed to enforce these contractual agreements effectively. The persistent practice by accredited registrars of accepting obviously false contact data from registrants and the recent actions by some large registrars to impose onerous and adhesive contractual restrictions on the availability of bulk Whois data are two examples of apparent non-compliance that ICANN has not adequately addressed.

ICANN management and its constituent bodies are aware of these concerns. Nevertheless, there is little indication that enforcement of these contractual agreements is a priority. The steps ICANN has taken are modest. For example, while ICANN recently created a central mechanism for receiving complaints about false Whois data, there is little transparency to complainants who often find it difficult to obtain information regarding what actions, if any, a given registrar or ICANN has taken in response. Additionally, there are reports that registrars have refused, in violation of their obligations under the RAA, to transfer domain name registrations after being so ordered by adjudicators under ICANN's Uniform Dispute Resolution Policy. Where there is a record of non-compliance with the terms of the RAA, ICANN must be more aggressive in exercising its authority to revoke a registrar's Accreditation.

Our Subcommittee has previously conducted hearings that examined privacy and intellectual property issues affecting Whois. The current discussion within ICANN involving "tiered access" and other proposals to change long-standing Whois policies have served to refocus attention on these issues. While we support efforts to protect privacy, it is imperative that the Internet's anonymity not serve as a shield for those who would harm children, consumers, network security, or the legitimate interests of intellectual property owners.

Given these concerns, we will appreciate your assessment of ICANN's efforts to enforce the Whois-related provisions of the RAA and your description of the specific steps the Department has taken to encourage ICANN, registrars, and registries to honor their contractual obligations. Additionally, an assessment of how the Department will address these concerns in any possible extension of the MOU will be greatly appreciated.

Another area of great interest to the Subcommittee is the increased role of the country code Top Level Domains (ccTLD's), the fastest-growing segment of the DNS. Many ccTLD's have adopted prohibitive Whois access policies that are substantially more restrictive than those that generally apply in the generic Top Level Domains (gTLD's), such as .com, .net, and .org.

We understand that ICANN currently has no contractual agreements with ccTLD's concerning access to Whois data or the related issue of dispute resolution in cybersquatting cases. While we are sensitive to the need to achieve consensus in seeking to bring ccTLD's under the umbrella of ICANN and we are encouraged by the recent approval by the ICANN Board of Directors of a new Country Code Name Supporting Organization (ccNSO), we were disappointed to learn that the ccNSO charter apparently seems to anticipate no meaningful role for ICANN in shaping ccNSO Whois and dispute resolution policies.

The Department is to be commended for seeking to promote the establishment of stable relationships between ICANN and the ccTLD's. However, we are troubled by ICANN's apparent inability to meaningfully contribute to accountability, transparency, and the establishment of a forum for the efficient resolution of domain name disputes in the formative stages of the relationship with ccTLD's.

In light of the foregoing, we ask that you provide us with your opinion of whether the ccNSO structure and charter adopted by the ICANN Board last month satisfy the MOU obligation of ICANN with regard to the ccTLD's; and, if not, what steps are required to meet those obligations. Additionally, we will appreciate your assessment of whether the ccNSO charter permits the development of binding policies on Whois or dispute resolution within the ICANN framework or whether other steps are necessary to

expand that scope.

Finally, we will appreciate your detailing for the Subcommittee the specific steps the Department has either taken or is in the process of implementing to encourage ccTLD's to adopt open Whois and dispute resolution policies. We are interested in understanding the full range of the Department's activities in this area, including activities internal to ICANN, such as participating in the Governmental Advisory Committee, as well as activities external to ICANN, including the use of bilateral discussions with other governments and the promotion of these policies through other intergovernmental organizations including WIPO and ITU.

In light of the imminent expiration of the current MOU, we would appreciate your addressing our concerns as soon as possible. Your responses will help the Subcommittee exercise its oversight responsibility and assist us in assessing the need for legislation to promote the accessibility, integrity, and comprehensiveness of domain name registrant contact information.

Thank you for your prompt attention to these important issues.

Sincerely,

LAMAR S. SMITH
Chairman, Subcommittee on Courts,
The Internet, and Intellectual Property

HOWARD L. BERMAN
Ranking Member, Subcommittee on
Courts, The Internet, and Intellectual
Property

[The response from Theodore W. Kassinger, on behalf of Secretary Evans, follows:]



**GENERAL COUNSEL OF THE
UNITED STATES DEPARTMENT OF COMMERCE**
Washington, D.C. 20230

September 11, 2003

The Honorable Lamar S. Smith
Chairman, Subcommittee on Courts,
the Internet, and Intellectual Property
Committee on the Judiciary
House of Representatives
Washington, D.C. 20215-6219

The Honorable Howard L. Berman
Ranking Minority Member, Subcommittee on
Courts, the Internet, and Intellectual Property
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515-6219

Dear Chairman Smith and Ranking Member Berman:

Thank you again for the opportunity to testify before the Subcommittee last week on the Department of Commerce's relationship with the Internet Corporation for Assigned Names and Numbers (ICANN) and enforcement of intellectual property rights protection in the domain name system. I appreciate the concerns that each of you and other members of the Subcommittee raised with respect to WHOIS accuracy and availability. I assure you that the Department has been an aggressive advocate of intellectual property rights in ICANN and other fora, actively promoting accurate and publicly available WHOIS data and dispute resolution procedures. Further, the Department recognizes that the WHOIS database plays a role for many different U.S. entities beyond intellectual property owners, all of which have an interest in an accurate and available WHOIS database.

On behalf of Secretary Evans, I also wish to take this opportunity to respond to your letter of August 8, 2003, to the Secretary. In that letter you asked several questions to which I directed my written and oral testimony at the hearing. I address each of those questions below.

1. What is the Department's assessment of ICANN's efforts to enforce WHOIS-related provisions of RAAs?

The Department believes that ICANN's new management understands the need for accurate and publicly available WHOIS data and is committed to improving the WHOIS system, including enforcement of the Registrar Accreditation Agreements (RAAs). More work clearly needs to be done in this area, however.

Two recent initiatives undertaken by ICANN are positive steps: the implementation of a centralized complaint process, and an annual WHOIS update requirement for accredited registrars. The "WHOIS Data Problem Reports" system has been operational for almost 12 months. ICANN is currently working to improve the functionality of this system, including making it easier for registrars to process and to report on the status of individual investigations and making the operations more transparent for persons submitting problem reports. The new "WHOIS Data Reminder Policy," which becomes effective in October, requires all accredited registrars to contact each registrant, at least annually, to confirm the accuracy of their contact information or to make necessary corrections.

These are steps in the right direction, but additional effort is required to secure substantial and uniform compliance with the goals for WHOIS accuracy that underlie the WHOIS provisions in the RAAs. We understand that ICANN also plans to hire new staff, which should improve the resources ICANN can devote to these issues.

2. What steps has the Department taken to encourage ICANN, registrars, and registries to honor contractual obligations?

The Department has monitored developments in the WHOIS arena closely since ICANN's inception and will continue to do so. The Department is particularly interested in the impact of the new complaint reporting process and annual WHOIS update requirement on improved accuracy.

Specifically, the Department has taken a number of steps to encourage ICANN, registrars, and registries to honor their contractual obligations, while focusing its efforts in the international arena primarily through the Governmental Advisory Committee (GAC), the World Intellectual Property Organization (WIPO), and the International Telecommunication Union (ITU). Most recently, the Department took a leadership role in the June 2003 educational workshop hosted by ICANN on WHOIS issues. The Department, through WIPO and the GAC, has actively encouraged the development of best practices for accurate and publicly available WHOIS data. Through the GAC, the Department has promoted a set of GAC "Principles for the Delegation and Administration of Country-Code Top Level Domains" for use by ICANN and ccTLDs which includes a principle to abide by ICANN-developed policies concerning the obtaining and maintenance of WHOIS-type data. The Department also has advocated the adoption of WHOIS-type registrant contact data and dispute resolution policies for Country-Code Top Level Domain (ccTLD) operators in U.S. bilateral trade agreements, including those recently concluded with Chile and Singapore.

In addition, the Department has formed an inter-agency working group to increase effectiveness of U.S. Government analyses and advocacy on these issues. Among other members, the working group is comprised of representatives from the Department of Commerce (U.S. Patent and Trademark Office and the National Telecommunications and Information Administration), the Department of Justice, and the Federal Trade Commission. This group is in the process of formulating a set of recommendations on WHOIS and related issues to be presented to the GAC during ICANN's meeting in October. The suggestions for WHOIS reform that emerged in the September 4th hearing will provide excellent guidance for this working group.

3. How does the Department plan to address intellectual property concerns in the MOU?

With respect to an extension of its Memorandum of Understanding (MOU) with ICANN, the Department intends to focus on the steps necessary for ICANN to evolve into an independent, stable, and sustainable organization well-equipped to fulfill its role in the technical management of the domain name and numbering system long into the future. While ICANN has made much

progress in this direction, it is essential in the next phase under the MOU to resolve certain fundamental issues associated with ICANN's long-term viability. Thus, the Department expects to negotiate an amended MOU that will include significant new obligations related to ICANN's organizational and financial stability, its relationships with key Internet stakeholders, and its timely introduction of new top-level domains. The importance and number of these essential undertakings leads us to conclude that the MOU likely must be extended for more than one year, coupled with milestones to ensure that ICANN achieves timely and steady progress. Consistent with the work the Department already has been undertaking, as well as the serious concerns expressed during the hearing last week regarding the lack of accuracy of the information in the WHOIS database, the Department also intends to work with ICANN, through MOU obligations and otherwise, to develop appropriate language to secure an acceptable level of WHOIS database accuracy.

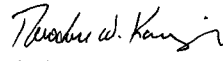
4. What is the Department's opinion on whether the ccNSO structure and charter satisfies ICANN's MOU obligation with regard to ccTLDs? What steps has the Department taken to encourage ccTLDs to adopt open WHOIS and dispute resolution policies?

The Department supports the formation of the Country-Code Names Supporting Organization (ccNSO) as a useful forum through which model agreements may be developed and other important issues, including WHOIS and dispute resolution procedures, may be discussed. The ccNSO, however, does not replace the MOU's requirement that ICANN enter into agreements with ccTLD operators.

Establishing stable agreements with the ccTLD operators is an important component of securing the future stability of the Internet. In the Department's view, the ICANN bylaws related to the ccNSO permit the ccNSO to make recommendations to the ICANN Board on WHOIS and dispute resolution policies for ccTLDs, which the Board could adopt. For such policies to be binding, however, the Department believes they would need to be included in an agreement between ICANN and individual ccTLD operators. The Department has actively encouraged ccTLDs to adopt open WHOIS and dispute resolution policies. As noted above, the Department has been and will continue to be very active in this area within the GAC, WIPO, the ITU, and bilateral negotiations.

Please be assured that the Department remains committed to ensuring that accurate WHOIS information is available to law enforcement, intellectual property rights holders, network operators, and consumers. We look forward to working with you on how best to achieve this objective.

Sincerely,



Theodore W. Kassinger

Mr. SMITH. In response, we will hear testimony that Commerce, one, intends to extend the MOU with ICANN for more than 1 year; two, recognizes the value of public access to online systems like Whois; and three, intends to include no affirmative steps in the MOU in an effort to improve ICANN's underwhelming enforcement record.

While Commerce intends to add a laundry list of seven milestones to assess ICANN's—excuse me, to assess ICANN's future performance, not one of these deals principally with Whois, contract enforcement, or intellectual property protections. This, too, at least in my judgment, is inexcusable.

If, as they say, the Commerce Department truly believes in a robust Whois, there is still time in the next MOU to address the well-established concerns of parents, consumers, intellectual property holders, and others who advocate for better Whois information. Rest assured, the Committee's attention to these issues will be judged by results, not by rhetoric.

That concludes my opening statement and the gentleman from California, Mr. Berman, will be recognized for his.

Mr. BERMAN. Thank you, Mr. Chairman, and thank you for scheduling this hearing today.

For the past three or more Congresses, this Subcommittee has examined the widespread problem of inaccurate and incomplete information in the Whois database. We have documented how inaccurate Whois data hampers law enforcement investigations, facilitates consumer fraud, impairs copyright and trademark protection, imperils computer security, enables identity theft, and weakens privacy protection efforts.

Recent events only serve to highlight the critical importance of accurate and complete Whois data. For several weeks last month, as the Chairman has mentioned, variants of the blazer computer worm disrupted or disabled approximately one million computers worldwide. Late last week, the U.S. Attorney in Seattle charged Jeff Parson, a Minnesota teenager, with writing and distributing lovesanB, a variant of the blazer worm that infected at least 7,000 computers. Accurate Whois data played a key role in identifying Jeff Parson as the culprit.

This investigation of Mr. Parson and the subsequent arrest made possible by the information on the Whois database represent just the latest example of the importance of an accurate Whois data. As did witnesses at many past hearings, witnesses today will provide further examples of the need for accurate Whois data while detailing its current unreliability. The importance of accurate and complete Whois data is, thus, well-documented. Well-documented, also, is the general unreliability and inaccuracy of the Whois data.

These facts beg the question. What should Congress do to remedy this serious problem? The time for cajoling relevant industry actors to act responsibly and self-regulate has expired. Former Chairman Coble and I contacted scores of registrars to gather information on their efforts to ensure accurate, complete Whois information. The handful of responses revealed little desire on behalf of registrars to take this issue seriously. We have tried through letters, hearings, and meetings to convince ICANN to deal with this

problem, but nothing of significance has happened. In fact, lately, there are indications of back-sliding.

Many times, we have encouraged the Commerce Department to vigorously advocate the demonstrated U.S. interest on this issue. Most recently, Chairman Smith and I, as he mentioned, asked the Commerce Department to address Whois issues in the process of renegotiating its Memorandum of Understanding with ICANN. These efforts also have proved wholly unsatisfactory. Unless Mr. Kassinger has a surprise announcement in store for us today, it appears the draft MOU fails to require that ICANN take steps to improve the accuracy or completeness of Whois data.

Rather than outlining any new Whois initiatives including—included in the Memoranda of Understanding, Mr. Kassinger's advance testimony only references several ongoing measures that have already proved woefully inadequate. Mr. Kassinger's testimony notes the existence of contractual obligations between ICANN and registrars and registrars and registrants providing for the accuracy and completeness of Whois data. However, a lack of enforcement has rendered these obligations meaningless. Registrars and registrants responsible for thousands of publicly-identified inaccurate or incomplete Whois entries ignore their obligations and fail to correct inaccuracies or incomplete Whois information. In the face of this, ICANN has only threatened one registrar with loss of accreditation.

While the Whois data problems report referenced by Mr. Kassinger is commendable, systems for self-reporting by victims should not relieve registrars of the obligation to proactively verify the accuracy of their Whois data. Prevention of crimes is more useful than setting up a mechanism for victims to identify themselves after the fact.

In conclusion, I am disappointed with the failure of both the marketplace and regulators to deal with this growing problem. A legislative solution seems necessary. Through section 303 of H.R. 2752, Ranking Member Conyers and I took one stab at crafting such a solution. I am open to other legislative approaches. And Mr. Chairman, if you are so inclined, I would welcome the opportunity to work with you in crafting an appropriate solution.

With that, I yield back. Thank you.

Mr. SMITH. Thank you, Mr. Berman. Our opening statements were not coordinated, but obviously, we have similar sentiments.

Let me just thank the gentleman from Texas, Mr. Carter, for being here today, as well as the gentleman from Wisconsin, for their interest in the subject at hand.

I will introduce our witnesses, and our first witnesses is Steven J. Metalitz, a partner in the firm of Smith and Metalitz, who specializes in intellectual property, privacy, E-commerce, and information law. Mr. Metalitz serves as Senior Vice President of the International Intellectual Property Alliance and is counsel to the Copyright Coalition on Domain Names. Formerly, Mr. Metalitz served as President of the Intellectual Property Constituency of ICANN as well as Vice President and General Counsel of the Information Industry Association. Mr. Metalitz is a Phi Beta Kappa graduate of the University of Chicago and a graduate of the Georgetown Law Center.

Our next witness is Benjamin Edelman, a fellow at the Berkman Center for Internet and Society at Harvard Law School. Mr. Edelman analyzes ICANN activities, operates the Berkman Center webcast, and develops software tools for real-time use in meetings, classes, and special events. He has authored articles regarding domain name issues, including the matter of expired domain names that are subsequently registered with false Whois data and used to sell pornography. Mr. Edelman graduated from Harvard College and is currently pursuing a law degree and doctorate in economics from Harvard.

Our third witness is James E. Farnan, the Deputy Assistant Director of the FBI's Cyber Division. Mr. Farnan was a Captain in the U.S. Air Force prior to joining the FBI in 1984. During his assignments in Houston, New Orleans, Las Vegas, and Washington, he has served as a civil litigator, general counsel, and drug and computer crimes investigator. Mr. Farnan received a bachelor's degree from Wheeling Jesuit University, a master's degree from Pittsburgh, and a J.D. from Temple School of Law.

Our final witness is Ted Kassinger, the General Counsel for the U.S. Department of Commerce. Prior to his current position, Mr. Kassinger was a member of the law firm of Vinson and Elkins. Mr. Kassinger received his undergraduate and law degrees from the University of Georgia.

Let me thank you all for participating, but before I get to that, let me say in Mr. Kassinger's defense, because he is going to get some tough questioning, that the Assistant Secretary who would have testified left 2 weeks ago, so we are catching him not exactly unawares, but he is not the original witness, so we may have to somewhat, Mr. Berman, mitigate our charges, but we will see on that.

In any case, we welcome you all, and just a reminder that we are limiting your testimony to 5 minutes and there will be ample time for us to ask you questions afterwards.

Mr. Metalitz, we will begin with you.

STATEMENT OF STEVEN J. METALITZ, PARTNER, SMITH AND METALITZ, LLP, AND COUNSEL, COPYRIGHT COALITION ON DOMAIN NAMES

Mr. METALITZ. Thank you very much, Mr. Chairman and Mr. Berman, Members of the Subcommittee. Thanks for the opportunity to testify on behalf of the Copyright Coalition on Domain Names representing a wide range of copyright owners.

CCDN's goal is to maintain public access to Whois data and to improve its accuracy and reliability because it is a key enforcement tool against online infringement. But as your opening statements clearly show, we are not the only ones who rely on Whois data. It's essential for protecting consumers online, as the FTC told you in last year's hearing before this Subcommittee. It's important for safeguarding network security and for law enforcement investigations. In fact, all Internet users, we believe, have a stake in keeping Whois data accessible and making it more accurate.

When this Subcommittee last looked at this issue 16 months ago, the accuracy and reliability of Whois data was deplorably bad. The first question is, has that changed? The short answer is, no. The

Whois database remains riddled with obviously inaccurate data, in some cases, the very same data that we cited to this Subcommittee last May. You have an expert witness here today in Mr. Edelman and I am sure he'll provide more detail about this problem.

Aside from the question of accuracy, Whois data has also become less accessible over the last year. For example, bulk access to Whois data, which all domain name registers are required to provide, has essentially been eliminated. The statement submitted by the International Trademark Association has some more details on this.

And finally, within the fastest growing part of the domain name space, the two-letter codes, the country code top-level domains, public accessibility of registrant contact data remains wildly inconsistent.

Now, what is ICANN doing about this problem? On paper, ICANN has established a good framework with three main features that are found in the registrar accreditation agreement that every domain name registrar must sign in order to go into the business of registering domain names in .com, .net, or .org.

First, domain name registrants consent in that agreement to collection of their contact data and its dissemination through Whois.

Second, the registrars are required to make that data available to the public via the web and through other means, such as bulk access.

And finally, registrants are required to provide complete and accurate data and to keep it current and they can lose their domain names if they don't do that.

Now, in practice, this system simply is not working. The basic problem remains that ICANN has never effectively enforced the contractual commitments that the registrars have made. Whois is a glaring example of this, although it's not the only one.

We see this as a fundamental flaw in ICANN's performance. The whole concept behind ICANN, to privatize management of the domain name system, depends on enforcing contracts that define what behavior is and isn't allowed. Much of ICANN's unfinished business that the Commerce Department has identified involves entering into additional agreements, making new contracts. So in this context, the question of whether ICANN is enforcing the agreements that it's already entered into isn't just a relevant question, it seems to us it's the central question in evaluating ICANN's performance.

ICANN now has a new structure. It has new leadership which is in a position to make a difference here. But the new leadership has inherited a gathering crisis of confidence about ICANN's willingness or ability to hold its contract partners accountable. How the ICANN leadership responds may determine ICANN's future prospects for success.

And I should add, I say this as a representative of a sector that supports ICANN. It participates actively in ICANN's processes. It believes ICANN has done many things right and it very much wants to see ICANN succeed.

But instead of prioritizing contract compliance and enforcement, ICANN has spent a lot of time and effort tinkering around the edges, and your opening statements refer to the complaint mecha-

nism that has been established. That has had only marginal impact on data accuracy. The fact that it has processed only 10,000 complaints over the last year is evidence of how peripheral it is, because this problem is much, much bigger than 10,000 domain names.

Then there was an ICANN task force on which I served that worked for 2 years looking at Whois issues, to try to get the registrars to step up and take some small steps to improve the quality of the data. But the final recommendations that emerged from this process were very modest and unlikely to be effective in tackling the real problem, and that problem is registrants who supply false contact data because they don't want to be accountable for their use of domain names or for what happens on their sites.

So how do we improve the situation? A year ago in our testimony, we said the buck stops with ICANN, and I think Subcommittee has correctly realized that that statement is incomplete. The buck really stops with the Department of Commerce and the impending expiration of the MOU is a critical juncture. We believe that now is the time for Commerce to obtain an ICANN commitment to contract enforcement and to write that commitment into the MOU with appropriate reporting requirements. This would be a big step forward for accountability on the Internet and for the healthy growth of E-commerce. We have a few other suggestions in our testimony that I would be glad to go into later.

Beyond oversight, Congress does need to consider legislative options, particularly if an ICANN contractual enforcement campaign never materializes or is ineffective, and the CCDN and others in the intellectual property community stand ready to work with the Subcommittee on the necessary changes.

Thank you again for your continued commitment to this important issue.

Mr. SMITH. Thank you, Mr. Metalitz.

[The prepared statement of Mr. Metalitz follows:]

PREPARED STATEMENT OF STEVEN J. METALITZ

Chairman Smith, Representative Berman, and Members of the Subcommittee:

Thank you for this opportunity to appear again to present the views of organizations of copyright owners on an issue that is vital to the enforcement of intellectual property rights in the online environment: ready access to accurate Whois data.

Before beginning my testimony, I would like to commend the subcommittee for its diligent and consistent focus on this critical issue over the past several years. The convening of this timely hearing, as well as the letter which Chairman Smith and Representative Berman sent to Secretary Evans last month on this issue, should be applauded by all who care about the healthy development of the Internet and e-commerce.

I am here today as counsel to the Copyright Coalition on Domain Names (CCDN), which has worked since 1999 on this issue. CCDN participants include leading industry trade associations such as the Business Software Alliance (BSA), the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and the Software and Information Industry Association (SIIA); the two largest organizations administering the performance right in musical compositions, ASCAP and BMI; and major copyright-owning companies such as AOL Time Warner and the Walt Disney Company.

The interests of copyright owners in preserving and improving access to reliable Whois data overlap considerably with those of trademark owners. Of course, many of the companies participating in CCDN, either directly or through their trade associations, own some of the world's most valuable trademarks and service marks. These companies invest heavily in defending these marks against infringements of

their intellectual property rights that take place online. Many of my remarks today apply at least as much to trademark concerns as they do to copyright matters.

This testimony will address four main questions:

- Why is real-time public access to complete and accurate Whois data essential?
- What is the current situation, and how has it changed since the Subcommittee's last hearing on the topic in May 2002?
- What is ICANN doing about the problem?
- What steps can be taken by the Department of Commerce—or by Congress—to improve the situation?

I. WHOIS: ACCURACY AND ACCESSIBILITY ARE CRITICAL TO E-COMMERCE AND ACCOUNTABILITY ONLINE

In its hearings over the past few years, this Subcommittee has compiled a comprehensive record, establishing why it is essential for the public to continue to have real-time access to contact data on domain name registrants—referred to as “Whois data”—and why the accuracy and currentness of this data is of the utmost concern. CCDN's primary focus is on the availability of Whois data for use in enforcing intellectual property rights online, but we know that is only part of a wider picture of the importance of accurate and accessible Whois.

As you know, copyright owners are currently battling 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: In your hearings last year, the Federal Trade Commission explained how they rely upon accessible and accurate Whois data to track down online scam artists, particularly in the cross-border fraud cases to which consumer protection agencies around the world are devoting increasing attention.
- Law enforcement: You will hear from a representative of the FBI today about the role Whois data plays in law enforcement activities generally. Public access to this data is critical to facilitate the gathering of evidence in cases of crimes carried out online, particularly in complex cybercrimes.
- 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 expert Security and Stability Advisory Committee recently 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.”

In practice, several of these well-established and vital uses of Whois data often overlap. Consider the troubling upsurge in cases of “phishing” or “corporate identity fraud.”

In recent weeks, hackers have 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, and that use domain names that are confusingly similar to the marks of these legitimate 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 chair-

man of the FTC recently 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.

II. WHOIS DATA QUALITY REMAINS POOR, AND ITS ACCESSIBILITY HAS DECREASED SINCE THE LAST HEARING

Of course, Whois cannot perform the critical functions I have just mentioned if the data it contains is false, incomplete, inaccurate or out of date. As the record of your May 2002 hearing amply demonstrated, at that time the quality of Whois data was deplorably bad. So has the situation changed since then? In a word, no.

The Whois database remains riddled with inaccurate data. This problem has been so well documented, particularly in the work of Ben Edelman of the Berkman Center, that there is little I need to add to his statistical studies and anecdotal examples. Suffice it to say that the specific example of obviously false Whois data that I cited to the subcommittee in my testimony almost sixteen months ago remains in the database today. Indeed, the Whois data for this domain name was even updated in December 2002—but apparently only to change the registrant’s “name” from “DVD Copy HQ” to “Rico Suave.” The address—1000 Lavaland Lane, Flabberville, CA—remains unchanged, and is obviously phony.

Accuracy of Whois data was the focus of last year’s hearing. But the accessibility of Whois data is also a critical issue, and on that front it is clear that conditions have worsened since last May. For example, one of the key mechanisms for providing public access to Whois—“bulk access”—is in a shambles.

Under their contractual agreements with ICANN, domain name registrars are required to make Whois data on their registrants available under license in bulk. This “bulk Whois data” is used by licensees to create value-added services, such as those marketed in connection with trademark searches. The “bulk Whois” obligation has never been popular with registrars, partly because the ICANN contract caps the license fees they can charge. But over the past year, registrars have taken matters into their own hands. They have evaded or defied their contractual obligations to ICANN, and have essentially eliminated bulk access to Whois data.

Some registrars have imposed onerous ancillary restrictions in their bulk access contracts; others have deleted most of the registrations from their database before making it available via bulk access; other registrars have just stopped offering these licenses, even though they promised ICANN they would do so. ICANN has done nothing to stop this. As a result, since so little of the total universe of Whois data can be obtained under bulk licenses, many of the value-added services have been withdrawn from the market.

The agreements with ICANN also require that registrars make Whois information available in response to queries from the public, including via the Web. To date, most registrars continue to make some Whois data publicly available on a retail basis. But too often the data available is incomplete, provided in non-standard formats, or simply not fully accessible. At the same time, many registrars advocate changes to ICANN policies that would allow them to significantly reduce public access to Whois data. If, in the near future, registrars decide unilaterally to restrict query-based public access, just as they have done with bulk access, we have very little confidence that ICANN would move to stop them.

I should add here that the observations above apply only to contact data on registrants in .com, .net or .org—the so-called “legacy generic Top Level Domains,” (gTLDs) for which Whois data is decentralized and held by each registrar, not by the centralized registry. While this still represents most of the domain name universe, the fastest growing part of that universe is found in the 243 “country code Top Level Domains” (ccTLDs), the two-letter domains like .us, .uk and .de (the German ccTLD, which is the world’s largest). The accessibility of registrant contact data

for the ccTLDs remains a patchwork quilt; while some ccTLD registries make this data readily available, others (including some of the largest ccTLDs) provide access to only very limited categories of data, or impose other restrictions on access that make it much more difficult to employ Whois.

III. WHAT IS ICANN DOING ABOUT THE PROBLEM?

Since the last hearing, and no doubt stimulated in great part by this Subcommittee's clear interest in the topic, ICANN has taken some steps to address the problems with Whois. However, they fall far short of an effective response to the reality of continued low data quality and reduced access.

The main step taken by ICANN management was to establish a centralized mechanism for receiving complaints of false contact data in Whois and passing these complaints along to registrars for action. ICANN even went so far as to threaten one registrar with the loss of its ICANN accreditation if it failed to respond to a handful of specific complaints. But it is very difficult to tell if the creation of this complaint mechanism has had any real impact on the problem of false Whois data. ICANN has released very few statistics on the operation of the complaint system, and we understand that some registrars take the position that they are not even obligated to report back to ICANN on what action, if any, they have taken in response to a complaint.

ICANN's Generic Name Supporting Organization (GNSO) has also undertaken a protracted process of examining Whois policy issues in an attempt to achieve consensus on what changes are needed. During its life span of over two years, the Whois Task Force conducted a massive online survey about how Whois was being used and what users expected from the system. It also issued a number of interim, draft and final reports. But in the end, the thousands of man-hours devoted to this effort produced remarkably little progress in addressing the problems plaguing Whois.

With respect to improving the accuracy of Whois data, in particular, the Task Force considered a number of proposed recommendations to require registrars to do more, in at least some circumstances, to increase the chances that the registrant contact data they are collecting is bona fide. Virtually all these proposals were rejected, deferred, or watered down to almost nothing. Inexpensive programs are available to registrars that will at least help screen out some false contact data; but registrars have shown little willingness to take even minimal reasonable steps to improve the quality of Whois data.

The final decision adopted by the Task Force and ultimately ratified by the GNSO and the ICANN Board boils down to this: registrars will be required to provide a reminder and an opportunity at least annually for registrants to update or correct their contact data in Whois. This extremely modest reform is likely to have little or no effect on the real problem: registrants who intentionally provide false contact data because they are making uses of domain names for which they do not want to be found.

Finally, with regard to the chaotic state of Whois accessibility in the ccTLDs, ICANN essentially seems to have thrown in the towel. The recent establishment of a country code name Supporting Organization (ccNSO) within the ICANN framework is certainly a positive step; but the scope of the ccNSO's jurisdiction is extremely circumscribed and appears to rule out any policy role for ICANN on Whois issues.

In short, the current stance of ICANN on Whois reflects an all too familiar theme. Within the gTLD environment, the contractual framework for a viable Whois policy is already in place. In order to be accredited by ICANN to register domain names, registrars are required to notify registrants about the need to provide accurate, complete and current contact data; to obtain their consent for making this data available to the public through Whois; to take steps to ensure that the data is in fact bona fide; to respond to reports of false contact data (including by canceling registrations that are based on false data); and to make specified Whois data available to the public, both in real time on an individual query basis, and through bulk access, under specified terms and conditions. The problem is—and the problem has long been—that these obligations have never been effectively enforced by the one entity with clear authority to enforce them: ICANN.

Copyright and trademark owners, and the organizations that represent them, support ICANN. We support the underlying concepts of this great experiment in private sector self-management of a critical Internet resource. Through the Intellectual Property Constituency, we have participated actively in the many and manifold ICANN policy development processes, including those related to Whois, and will continue to do so. Much can be accomplished through dialogue in the ICANN frame-

work, and we remain deeply engaged in that dialogue. But it is essential that ICANN understand that its failure to effectively tackle the problems plaguing Whois—which translates, to a great extent, to its failure to effectively enforce the contracts it has entered into with registrars and registries—is severely testing its continued support and engagement.

Under new leadership and with a reformed structure and charter, “ICANN 2.0” is laying great plans to take more comprehensive steps to ensure stability and security in the Domain Name System. But all those plans depend upon the development and implementation of voluntary agreements with key players. Unless and until ICANN can instill greater confidence in its approach by effectively enforcing the agreements it has already entered into, its future plans, and indeed perhaps its future viability, will remain shrouded in uncertainty.

The success of the ICANN model for private sector, consensus-based management of the DNS depends upon scrupulous observance of the contractual undertakings which embody the policies developed by ICANN. The widespread failure of registrars to abide by those undertakings with respect to Whois, and the even more disturbing failure of ICANN to enforce those undertakings vigorously, does not bode well for the success of the ICANN model. Accreditation by ICANN as a domain name registrar is not an entitlement, but a privilege regulated by contract; and ICANN has not effectively used the power to revoke accreditation in order to achieve higher levels of compliance with contractual commitments.

IV. WHAT DOC SHOULD BE DOING TO IMPROVE THE SITUATION

Mr. Chairman, in our testimony at last year’s hearing, we said that, with respect to the problems of accuracy and integrity of the Whois database, “the buck stops with ICANN.” I believe that you and Mr. Berman have correctly recognized that this statement is incomplete. In many respects, the buck stops with the Department of Commerce, which oversees and manages the relationship with ICANN as part of the overall task of managing the Domain Name System. That relationship is at a critical juncture with the impending expiration of the Memorandum of Understanding between the Department and ICANN. We believe that your letter of August 8 to Secretary Evans correctly framed many of the key questions that need to be answered in fashioning the terms and conditions under which that MOU will be extended past September 30.

The staff of the Department of Commerce, and the other US government representatives who have participated in ICANN, have certainly played a constructive role in encouraging ICANN to step up to the issues of Whois availability and accuracy. We believe that they can and should do more. Here are some specific proposals which we urge DOC to consider.

- (1) *Obtain an ICANN commitment to contract enforcement, embodied in the MOU.* As I have already noted, the ineffectiveness of ICANN’s enforcement of its agreements with registrars and registries has repercussions far beyond the issue of Whois. It is long past time for ICANN to commit to devoting adequate resources to the contract compliance, monitoring and enforcement functions, and to providing greater transparency in its enforcement efforts. In the MOU, ICANN should make this commitment, and also agree to much more detailed reporting on its efforts to ensure that registrars and registries meet their responsibilities with regard to Whois data quality and accessibility, among other issues. If ICANN demonstrates its readiness to prioritize contract enforcement activities, DOC should in turn be supportive of proposals for a moderate increase in the per-registration ICANN assessment fee collected by gTLD registrars, if this is needed to achieve adequate funding.
- (2) *Keep a close eye on the Whois policy development process.* Following a successful and informative set of workshops on Whois at its recent Montreal meeting, ICANN is embarking on a new phase of policy development activities with respect to Whois and privacy issues. While a number of issues could legitimately enter into this debate, these activities will be most constructive if they focus on incremental steps, particularly in improvement of the quality and accuracy of Whois data, rather than on more sweeping changes that could reduce or restrict access to Whois data and thus undermine the transparency and accountability that Whois can provide. ICANN’s CEO has already stressed the important role of governments in the reorganized ICANN framework for developing policy. The U.S. government should step up to this role in the case of Whois.
- (3) *Build an international constituency for Whois within the ICANN Governmental Advisory Committee (GAC).* Ordinary Internet users all around the

world will benefit from the increased transparency and accountability that Whois can provide if the quality of its data is improved and if ready access to the data is maintained and enhanced. The governments that participate in the GAC will also benefit, since public access to accurate Whois data facilitates key government functions such as law enforcement, consumer protection, and protection of children from inappropriate online activities. However, these broader public safety and governmental concerns are not always voiced within the GAC, whose participants can be influenced by other bureaucratic and ideological goals. The US government participants in the GAC should make it a priority to build international support for the role of Whois, and to promote awareness of the social costs of restricting access to Whois or failing to address the accuracy issue.

- (4) *Push for best practices on ccTLDs.* Although ICANN may not be in a position at present to develop binding Whois policies for ccTLDs, there is much that DOC can do, including within the GAC, to encourage other governments to move their local ccTLD registries toward improved policies. The “GAC Principles for the Delegation and Administration of Country Code Top Level Domains,” adopted in 2000 as a result of U.S. leadership, provide a good starting point for this discussion, and their underlying approach should be maintained. DOC should also consider how our own ccTLD registry—.us—could be promoted as a model for others to emulate. The same agency within DOC both leads the US delegation to the GAC and administers the registry contract for .us; coordination between these two roles should be enhanced.
- (5) *Advocate within intergovernmental organizations for accessible and accurate Whois.* The World Intellectual Property Organization (WIPO) is a key forum in this regard. Its “ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes,” adopted in 2001, offer an excellent resource for ccTLDs seeking to adopt sound Whois policies. Because of the importance of Whois as an intellectual property enforcement tool, WIPO’s increased focus on enforcement best practices provides a good opportunity to reinforce the value of accurate and accessible Whois. In addition to WIPO, the International Telecommunications Union (ITU) is becoming increasingly active on issues relating to the domain name system (DNS). While it would certainly be counterproductive for ITU to usurp or supplant ICANN’s role, to the extent the ITU is involved, the USG should be engaged and should advocate for sound policies that promote the transparency and accountability of the DNS.
- (6) *Be alert for other international fora.* Promotion of sound Whois policies should be integrated into DOC’s trade policy, e-commerce, and other international activities. With regard to ccTLDs, future trade agreements should build on and improve the provisions of the Singapore and Chile Free Trade Agreements that call on signatories to promote Whois access and accuracy, as well as alternative resolution systems for domain name disputes within their national registries. DOC and other Executive Branch agencies should also consider how best to use fora such as the World Trade Organization to reduce impediments to public access to accurate Whois data, bearing in mind the obligation of all WTO member states to provide effective mechanisms against infringements of intellectual property rights, including those taking place online.

V. LEGISLATIVE OPTIONS

Finally, although we recognize that this is an oversight hearing, we urge the subcommittee to also consider legislative changes that could advance the cause of accessible and accurate Whois data. Some relatively simple steps could help. For example, online criminals often submit false Whois data to evade detection when they set up an Internet site for use in carrying out piracy, fraud, or other offenses. It would make sense to adopt a provision increasing the potential sentence of a person convicted of carrying out a federal crime online, when it is proven that false contact data was intentionally submitted in furtherance of the criminal scheme.

The more complex challenge is to enhance existing incentives for registrars and registries to handle Whois data more responsibly. It is obvious that existing incentives are insufficient. Too many registrars and registries do far too little to screen out false contact data at the time of submission; to verify or spot-check contact data that is submitted; or, at a minimum, to respond promptly and effectively to complaints of false contact data, including by canceling the domain name registrations which the false data supports. We hope that more aggressive and effective enforcement by ICANN will make a difference. But if it does not, or if the needed ICANN

enforcement campaign is not forthcoming, Congress must seriously consider stepping in to provide the incentives by statute. Should this occur, CCDN would be pleased to work with this Subcommittee on appropriate legislative options.

Thank you once again for the opportunity to testify today. I would be pleased to answer any questions.

Mr. SMITH. Mr. Edelman?

STATEMENT OF BENJAMIN EDELMAN, FELLOW, BERKMAN CENTER FOR INTERNET AND SOCIETY, HARVARD LAW SCHOOL

Mr. EDELMAN. Chairman Smith, Ranking Member Berman, Members of the Subcommittee, in the interests of full disclosure, let me pause to add one sentence to my biography. I previously worked for ICANN as a consultant, primarily making their meetings available for viewing and participation over the Internet, but to be sure, also on some substantive issues, including even Whois. Suffice it to say that we have parted ways and I am here for myself and for the Berkman Center at Harvard, not for ICANN. But let no one think I have anything to hide.

Like Members of the Subcommittee, I've followed Whois accuracy problems for, at this point, more than a decade. My recent research has attempted to bring the issue into a new focus by finding some of the bad apples, and to the extent I am able, calling attention to them.

Indeed, I have published lists of many thousands of domains with invalid Whois data, as well as what information I can find about their likely registrants and about the registrars who continue to serve them. I want to note that this reporting is a poor substitute for real efforts at enforcement of the sort I'll propose in a moment and of the sort that took place yesterday in Florida, when notorious false Whois registrant John Zuccarini was arrested. Ultimately, even if I write an article about a registrant, the registrant keeps the domain and the problem remains.

With that, let me review the key findings of my research and the suggested solutions in my testimony.

As to what's going wrong, I see two sets of problems. First, registrants face no meaningful incentives to provide accurate Whois data. Registrants can submit blatantly invalid data without fear of monetary or other sanction, and so they do.

Second, registrars face no meaningful incentives to demand accurate Whois data from registrants, to be sure, their customers. What few incentives registrars might face are toothless, infrequently and arbitrarily invoked, and, therefore, ignored.

The result is that in terms of accuracy, when compared with other compilations of public data, like drivers' licenses and trademark registrations, the Whois database is substantially fiction.

With these diagnoses in mind, let me suggest five policy responses.

First, a reduction in the leniency of opportunity to cure intentionally invalid data. At present, when a registrant is caught with invalid Whois data, the registrant can fix it without penalty. Sounds great, but so long as this is the policy, why would a registrant ever provide correct data in the first place? Some form of sanction, be it forfeiture of the domain or payment of a fine, is necessary to discourage intentionally invalid entries.

Second, for registrants with multiple domains with intentionally invalid data, forfeiture of all domains when any are to be canceled. For a registrant with, say, 5,000 domains, it's laughable to seize just one. The registrant will never notice and certainly will never much care.

Third, statistically valid surveys of registrars' Whois accuracy with public reporting of each registrar's performance. Registrars with poor record can expect a sort of public humiliation, at the very least, invitations to explain themselves before Committees like this one.

Fourth, improvements in transparency of ICANN's Whois complaint system. At present, the status of Whois complaints is largely unknown. There is no systematic way to track which registrars act on complaints and which ignore them. Publishing the complaints and their dispositions would be beneficial to all, would allow researchers, the press, and this Subcommittee to know which registrars are doing best, and to be sure, which worst at Whois accuracy.

Finally, if reporting and suggestions three and four didn't succeed in inspiring registrars to demand accurate data from their customers, ICANN or the Department of Commerce could impose financial and other penalties on registrars with the worst Whois accuracy records. It may sound far-flung, but it's actually hardly unprecedented. ICANN's contracts with registries already impose financial sanctions for poor performance.

I appreciate the opportunity to offer these suggestions and I look forward to working with the Subcommittee in the future.

Mr. SMITH. Thank you, Mr. Edelman.

[The prepared statement of Mr. Edelman follows:]

PREPARED STATEMENT OF BENJAMIN EDELMAN

Chairman Smith, Ranking Member Berman, Members of the Subcommittee:

My name is Benjamin Edelman, and I am a fellow at the Berkman Center for Internet & Society at Harvard Law School, where I write software to study the Internet. Among my research interests is the Internet's domain name system, and I have written a series of articles about flaws in the Whois system, about domain name registrants who exploit these flaws, and about possible means of detecting and preventing such exploits. My full biography and publication list are available at <http://cyber.law.harvard.edu/edelman>.

In the interests of full disclosure, let me pause to note that I previously worked for ICANN. I designed and operated webcasts of fully a dozen ICANN's meetings – so that anyone interested could watch, read, and even ask a question from home or office, without traveling to a far-flung meeting site. In 2000-2001, I also briefly served as a consultant to ICANN as to technical issues associated with the introduction of new top-level domains as well as with certain security and competition concerns.

Today the subcommittee considers the accuracy of the Whois database, and the role of the Department of Commerce, ICANN, registries, and registrars in assuring the accuracy of Whois data.

My bottom line:

As the DNS is currently structured, registrants are under only an honor system to provide accurate Whois data. Meanwhile, it makes no economic sense for registrars to enforce Whois accuracy. The result is that in terms of accuracy, when compared with other compilations of public data (such as driver's licenses and trademark registrations), the Whois database is substantially fiction.

Despite years of inquiry by this subcommittee, in addition to numerous ICANN working groups and other discussions, intentionally invalid Whois data remains widespread. But failure to solve this problem so far doesn't mean the subcommittee must give up. Instead, new efforts at detection could better find invalid domain names, while new incentive systems assure that registrants provide accurate data and that registrars confirm that they do so.

My specific suggested incentives include 1) a reduction in the lenience of opportunity to "cure" intentionally invalid data, 2) for registrants with multiple domain names with intentionally invalid data, forfeiture of all domains when any are to be cancelled, 3) statistically valid surveys of registrars' Whois accuracy, with public reporting of each registrar's accuracy, 4) public reporting of Whois accuracy complaints and their dispositions, and 5) financial and other penalties to registrars with poor Whois accuracy records.

Scope of the Problem of Invalid Whois Data

The Internet's domain name system (DNS) currently includes approximately thirty million domain names within the top-level domains of .COM, .NET, and .ORG. Under ICANN policy, passed on to domain registrants through contracts via registry and registrar, each of these domains must report the name, address, telephone number, and email address of its technical and administrative contacts, as well as the name and address of the its registrant. This information must be published via the so-called "Whois" database operated by domain name registrars.

It has long been known that a large number of domain names offer invalid Whois contact information. In some instances, the invalidity may be unintentional; registrars' data systems occasionally corrupt registrant contact information, and registrants (especially non-native English speakers) might misunderstand registration forms. In general, though, invalidity is thought to be intentional, reflecting registrants' desire to keep their identities confidential. This inference is particularly strong when Whois data is obviously intentionally invalid ("123 Main Street" or "0 Does Not Exist Lane"), when invalid Whois data is combined with controversial content (pornography, cybersquatting, etc.), or when the invalid information and associated web sites are clearly the work of sophisticated registrants.

In the past, some have attributed Whois accuracy shortfalls to difficulty in determining whether specified addresses are valid. After all, if a registrar cannot determine if a given address is accurate, the registrar cannot enforce accuracy requirements. However, automated systems are increasingly well able to cross-check registrant name, address, and postal code, all with minimal delay and low cost, at least as to registrations in industrialized countries. A new service called Fraudit (from a DNS service provider called Alice's Registry¹) performs precisely these functions, using only publicly-available databases. Credit card verification software typically uses similar methods, and registrars have been using card verification software for some time in order to reduce "chargeback" penalties and confirm validity of customer credit cards. However, I know of no registrar currently using these methods to prevent invalid Whois data.

Using a variety of methods of locating suspicious registrations, my prior research identifies thousands of domains with intentionally invalid Whois data. For example, in my May 2002 *Large-Scale Intentional Invalid Whois Data: A Case Study of "NicGod Productions" / "Domains For Sale"*,² I identified a total of 2,754 domains registered by a single registrant – but using addresses in at least ten countries, registered via at least eleven registrars. Similarly, my January 2003 *Large-Scale Registration of Domains with Typographical Errors*³ reports more

¹ <http://www.ar.com>

² <http://cyber.law.harvard.edu/people/edelman/invalid-whois>

³ <http://cyber.law.harvard.edu/people/edelman/typo-domains>

than 8,800 domains registered by a single registrant using at least six pseudonyms, using addresses in at least six countries, and using at least four registrars.

Intentionally invalid Whois data is often associated with other controversial registration practices. This is perhaps not surprising – after all, registrants with something to hide are particularly likely to conceal their true contact information. My *NicGod* research found clear evidence of bulk registration of domains previously used by other registrants, then allowed to lapse (typically mistakenly, e.g. by administrative error), subsequently captured by NicGod, which then attempts to resell them to their original registrants after markups on the order of 5000%. My *Typographical Errors* research found registrations of strings that are small variations on well-known marks (e.g. cartoonneetwork.com [sic]), and the resulting domains were typically redirected to sites offering pornography, online gambling, filesharing, or other controversial materials. These are troubling practices – practices which force small business owners to pay thousands of dollars to retain the domains they previously used, and practices which expose Internet users to pornography as a penalty for small mistakes in typing URLs.

Incentives for Registrants to Provide Accurate Data

That registrants provide invalid Whois data should perhaps come as no surprise. After all, domain name registrants have only limited incentives to provide accurate Whois data.

1. Accurate Whois data is not necessary in order to pay for a domain name. Even when contact information is cross-checked with credit card records at the time of domain registration, it is typically possible to modify contact information subsequent to registration.
2. Registration agreements, typically accepted by registrants by pressing an “I agree” or similar button during the domain name registration process, oblige a registrant to provide accurate Whois information. But few registrants typically read these agreements, and the format of these agreements rarely places special emphasis on Whois accuracy.
3. Even when registrars send periodic reminders that Whois data must be kept up to date, as is required under ICANN’s Whois Data Reminder Policy,⁴ registrants are likely to ignore the reminders. This too is no surprise – particularly since Whois reminders are widely thought not to be supported by active investigation or enforcement.

⁴ “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.” <http://www.icann.org/registrars/wdrp.htm>

4. When a registrar receives a complaint as to the accuracy of a registrant's Whois data, the registrar typically grants the registrant an opportunity to cure the problem by correcting the invalid entry. Anticipating this opportunity, a registrant need not offer accurate information in the first instance. Instead, the registrant can provide invalid Whois data, to be corrected only upon complaint. In addition, some registrants provide a series of invalid contact names and addresses, a problem recently faced by staff of the OECD.⁵

In short, the current registration scheme fails to set incentives for registrants to provide accurate Whois data. The system provides no incentives for registrants to provide accurate data in the first instance – for registrants always receive an opportunity to cure invalid entries, without penalty. Furthermore, the system allows bulk registrants to sacrifice a disputed domain rather than share their true identities – for domain cancellations are limited to the specific disputed domains and do not extend to other domains registered by the same registrant using the same invalid Whois data.

The following modifications would correct these incentive problems

1. When a registrant's Whois data is found to be intentionally inaccurate, penalize the registrant in some way before (or instead of) offering an opportunity to correct the error. The penalty could consist of charging a fee for investigation, or forfeiting some period of prepaid registration service.
2. When a given domain name is to be cancelled for offering invalid Whois data, also cancel all other domain names registered with identical invalid Whois data.

Incentives for Registrars to Assure Accurate Data

Registrars' failure to enforce Whois accuracy is also predictable, for registrars face equally limited incentives to provide accurate Whois data.

1. Registrar contracts with ICANN oblige registrars to include certain language in their contracts with registrants, asking registrants to provide accurate Whois data.⁶ But this requirement extends only to language in registration agreements – not to actual efforts at enforcement. Neither do other sections of registrar contracts with ICANN require specific enforcement procedures as against registrants who provide invalid Whois

⁵ "Cybersquatting: The OECD's Experience and the Problems It Illustrates with Registrar Practices and the 'Whois' System" <http://www.oecd.org/dataoecd/46/53/2074621.pdf>

⁶ "Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions ..." <http://www.icann.org/registrars/ra-agreement-17may01.htm#3.7.7>

data.⁷ In fact, ICANN specifically allows registrars to maintain domains even in the face of intentionally invalid Whois data constituting a material breach of the domain registration agreement.⁸

2. For failure to assure Whois accuracy, registrars face only a toothless sanction from ICANN, and ICANN isn't even making meaningful use of this approach. Pursuant to ICANN's April 3, 2003 advisory to registrars,⁹ and as took place in September 2002,¹⁰ ICANN may present a registrar with a formal notice of breach if, in ICANN's view, the registrar "appears to routinely ignore reports of inaccurate and incomplete contact data in its Whois database." However, only one such notice has been issued to date; it reported inaccuracies in only seventeen domains; its recipient was a registrar not typically thought to harbor particularly egregious cases of invalid Whois data; the only resulting sanction was brief public embarrassment for the registrar, without financial penalty. Registrars are unlikely to respond to such sporadic enforcement by ICANN.

In contrast, registrars face clear incentives to allow inaccurate Whois data.

1. The costs of inaccurate Whois data fall not on registrars but on others – on law enforcement officials, on consumers, and on those wishing to pursue copyright, trademark, and other claims against domain name registrants.
2. A registrar that enforces Whois accuracy requirements faces increased costs relative to a registrar that ignores Whois accuracy. Increased costs include staff time to seek out errors and respond to customer complaints, as well as software to automate these processes.
3. A registrar that enforces Whois accuracy requirements may face lost revenue by driving certain customers to other registrars. In particular, large registrants with systematic intentionally invalid contact information (such as the registrants described in my *NicGod* and *Typographical Errors* research) are likely to select registrars that allow or tolerate invalid contact information.

The following policy changes would correct these incentive problems:

1. ICANN could commission audits of Whois accuracy, using statistically valid methods to examine a significant sample of domains. Results would be tabulated and published on a per-registrar basis, allowing comparisons of Whois accuracy among registrars.

⁷ e.g. "take reasonable steps to investigate" – <http://www.icann.org/registrars/ra-agreement-17may01.htm#3.7.8>

⁸ <http://www.icann.org/announcements/advisory-03apr03.htm>

⁹ <http://www.icann.org/announcements/advisory-03apr03.htm>

¹⁰ <http://www.icann.org/correspondence/touton-letter-to-beckwith-03sep02.htm>

2. ICANN could use the results of Whois accuracy audits to present registrars with formal notices of breach of their contracts with ICANN.
3. If formal notices of breach fail to encourage registrars to improve their performance on Whois accuracy audits, ICANN could implement a system of graduated financial sanctions, consistent with ICANN's practice for registry service level agreements.¹¹
4. ICANN could post periodic statistics as to Whois Data Problem Reports, Registrar Problem Reports, and registrars' actions taken in response to these complaints.

All registrars would face these policy changes simultaneously and equally. Across-the-board enforcement of Whois accuracy would prevent registrants from switching registrars to avoid Whois enforcement efforts.

Privacy Concerns Reflect Misguided Overemphasis

In response to calls for increased Whois accuracy and enforcement, some have raised privacy concerns.¹² Their typical worry is that an emphasis on Whois accuracy would purportedly prevent individuals from registering domains for purposes that are in some way controversial yet simultaneously commendable (e.g. political dissent, whistle-blowers, or other anonymous speech).

Polymakers rightly encourage the use of the Internet for activities legitimately requiring anonymity. However, such activities are in no way incompatible with accurate Whois data. Domain registrants who wish to keep their name and address confidential can register names through one of several third-party services specializing in privacy protection¹³ or can register names through an attorney or other representative. It is not necessary to sacrifice Whois accuracy in order to preserve the possibility of anonymous publication on the web.

Distinct from the privacy concerns typically offered in response to calls for Whois accuracy, are concerns as to publication of truthful email addresses, for fear of receiving unsolicited email. In the past, such emails have included offers from registrars and web hosting companies. More recently, email worms and viruses have proven particularly disruptive. I am sympathetic to these concerns, but the proper response is not to discard all calls for Whois accuracy. Indeed, email concerns in no way lessen the need for accurate registrant name, address, and telephone information. Instead, those who find bulk email problematic can route their email through any of various mail filtering services, or can rely on temporary "alias" email addresses. Certain registrars already offer this email alias feature,

¹¹ e.g. <http://www.icann.org/lds/agreements/name/registry-agmt-apppe-02jul01.htm>

¹² e.g. Electronic Privacy Information Center – Whois. <http://www.epic.org/privacy/whois/>

¹³ e.g. GoDaddy's Private Registration service, https://registrar.godaddy.com/dbp.asp?isc=&se=%2B&pl_id=1&prog_id=GoDaddy

typically at no additional charge.¹⁴ In any case, recent research indicates that Whois records are not a significant source of spam.¹⁵

Trends in Registrar Compliance with ICANN Policies

I understand that the subcommittee is also concerned about the possibility that certain registrars systematically tend not to comply with relevant ICANN policies. In particular, despite obligations under the Registrar Accreditation Agreement, certain registrars apparently ignore selected UDRP judgments calling for transfer of domains away from the registrars and their registrant customers. New York attorney Martin Schwimmer publicly raised this issue in a blog entry of June 4, 2003,¹⁶ and I have subsequently attempted to quantify the scope of the problem in my *Compliance with UDRP Decisions: A Case Study of Joker.com*.¹⁷ I have found significant evidence that registrar Joker.com, perhaps among others, systematically fails to abide by its contractual obligation to transfer domains subsequent to orders received from UDRP panels.

To assure that registrars comply with their contractual obligations to ICANN, ICANN could establish a procedure for formally receiving, processing, and acting on complaints against registrars, ultimately upon threat of termination of an offending registrar's Accreditation Agreement. At present, ICANN's investigative procedures are ad hoc, and many complaints therefore fall through the cracks – with extended delays before ICANN takes action, if it does so at all. A more formal method of passing complaints to ICANN – complete with web-based publication of complaints, status, and disposition – would assure that ICANN acts promptly and transparently in resolving these situations.

The Special Problems of .US

The Department of Commerce has a special ability to shape policy in the United States' country-code top-level domain, .US. In particular, the DoC has a direct contractual relationship with .US registry Neustar, allowing DoC to directly specify .US policies. (In contrast, DoC's influence over policies in .COM, .NET, etc. require passing through DoC's Memorandum of Understanding with ICANN and subsequently through ICANN's policy-making process.) In this context, it is particularly desirable to assure that .US Whois rules and associated registration policies are fully in order.

¹⁴ e.g. <http://www.namescout.com/master/privacyfeatures.asp>

¹⁵ "Addresses posted in ... Whois domain name registries ... did not receive any spam during the six weeks of the investigation." <http://www.ftc.gov/bcp/online/pubs/alerts/spamairt.htm> "Domain name registration does not seem to be a major source of spam."

<http://www.cdt.org/speech/spam/030319spamreport.pdf>.

¹⁶ <http://trademark.blog.us/blog/2003/06/04.html#a646>

¹⁷ <http://cyber.law.harvard.edu/people/edelman/udrp-compliance>

.US Whois Policy

Neustar's .US Policies page¹⁸ makes no mention of a .US policy as to Whois accuracy or registry procedures for assuring Whois accuracy. NeuStar's Registration Review Policy¹⁹ references "Accuracy of information," but places this section at heading six on page three of a PDF file (easy for registrants to miss) and fails to use the word "Whois" to make clear to registrants what specific information is at issue. Improvements in these areas are necessary to assure .US's position as a leader in Whois accuracy.

.US Nexus Requirements

Closely related to .US Whois rules are .US nexus requirements for registration. Under the .US Nexus Requirements,²⁰ .US domains may be registered only by 1) US citizens or residents, 2) US entities or organizations, and 3) foreign entities or organizations with a bona fide presence in the US. In practice, however, .US domains are registered by a variety of entities meeting none of these criteria. Furthermore, these entities often register a large number of domains – as many as 800 per registrant, in my research – and their domains often infringe on the marks of others. These practices are documented in my *Survey of Usage of the .US TLD*.²¹ However, despite discussion list coverage of this research, as well as numerous personal emails from concerned citizens to staff at the Department of Commerce and at Neustar, I gather these registrations remain in effect, in many instances with new invalid Whois information replacing the old.

If existing procedures fail to separate US from non-US registrants – on the basis of what could initially have been presumed to have been truthful registrant contact information – their ability to perform the more subtle task of separating valid Whois contact data from invalid entries ought to be very much in question. Here too, improvement likely requires setting appropriate incentives – requiring Neustar to face a penalty when it allows the registration of scores of domains with invalid Whois data or with invalid nexus qualifications.

The Unavailability of the .US Zone File

The Department of Commerce's agreement with Neustar apparently fails to provide the public with access to the .US zone file (the list of all registered .US domain names). Zone files are essential for conducting research as to trends in domain registrations, and public access to zone files is therefore a cornerstone of all ICANN contracts with gTLDs. However, Neustar reports that the DoC has failed to provide for such access under its .US contract with Neustar, and Neustar staff refuse to distribute the file to the public until the DoC and Neustar agree on terms for doing so. As a result, research and public critique of .US registrations and policies are rendered considerably more difficult, and it was

¹⁸ <http://www.nic.us/policies>

¹⁹ http://www.nic.us/policies/docs/registration_review_policy.pdf

²⁰ http://www.nic.us/policies/docs/ustld_nexus_requirements.pdf

²¹ <http://cyber.law.harvard.edu/people/edelman/dotus>

only with considerable additional effort that I was able to conduct the *Survey* referenced above.

Lack of Related Efforts by the .US Policy Council

.US policy is to be set in consultation with a .US Policy Council, formed by Neustar in 2002. However, the status of this Council is unclear, with no meeting minutes posted since January 2003.²² My sense is that this period has brought a similar lack of forward progress on .US Whois accuracy, nexus requirements, zone file availability, and other .US policy issues.

²² <http://www.neustar.us/policycouncil>

Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale"

[[Overview](#) - ["Domains For Sale"](#) - [Types of WHOIS Errors](#) - [Specific Domains](#) - [Summary Statistics](#) - [Conclusions](#) - [Policy Implications](#) - [Motivation](#)]

Overview

In recent years, many Internet users have become aware that domain name registrants do not always offer accurate contact information. The distributed "WHOIS" database storing and distributing this contact data is generally thought to be important for correcting technical errata, resolving disputes over domain name allocation, and holding web site operators responsible for the content they distribute. A series of contracts, from ICANN to registrars to registrants, requires that contact data be complete and accurate, but nonetheless certain registrants fail to properly provide the required contact information.

While many WHOIS errors likely result from accidental error in data entry or data processing, certain registrants have been found to intentionally provide systematically inaccurate contact information to registrars for inclusion in the WHOIS database. Such fraud can include the entry of invalid street addresses and phone numbers, i.e. contact information that in fact reaches no one, or it can instead offer as the purported registrant of a domain some third party in fact wholly unrelated to the domain.

In recent research, I have documented 2754 domains reregistered by one particular firm known for its widespread use of invalid WHOIS contact information. The majority of these domains redirect users to a single web page displaying a list of links to content that is, by and large, unrelated; the remaining domain names provide access to sexually-explicit images. While this research is by no means exhaustive -- other firms likely follow similar registration practices, and still others make numerous invalid registrations and reregistrations that no doubt differ in various ways -- a review of these specific registrations as well as their general characteristics may be helpful in understanding the behavior at issue.

Note that this research is focused specifically on large-scale domain registrations. I do not address the questions of privacy, spam, and consumer protection raised by publication of individual registration data in the WHOIS database.

A Case Study: "Domains For Sale" Reregistrations by an Undetermined Registrant

Recent testing reflects that a firm calling itself "NicGod Productions" and "Domains For Sale" (henceforth, "NicGod") operates at least 2754 domain names that by and large redirect to a page that offers a list of links unrelated to the requested domain. A subset of NicGod's domains offer sexually-explicit images on a paid subscription basis.

NicGod's 2754 domains include a wide variety of character strings. The vast majority of domain names explicitly suggest specific content other than what is present on the subsequent list of links -- for example, [angry-kids.com](#), [californiastateuniversity.com](#), [doctorjohn.com](#), [polygram-us.com](#), [reform-party-usa.org](#), and [winthrop-police.com](#).

It seems that most or all of NicGod's domains were previously held by other registrants. According to archive.org, at least 1844 (67.0%) of NicGod's domains previously offered HTML titles suggesting the availability of other content, precisely indicating that the domains were previously put to another use before registration by NicGod. Some 246 (8.9%) of NicGod's domains continue to be listed in Yahoo, in categories reflecting the prior availability of content other than the current NicGod listing of links. Similarly, some 2170 (78.8%) of NicGod's domains are mentioned on one or more other pages, as reported by Google; these many outside references further suggest that the NicGod domains previously hosted other content. In this regard, NicGod's registration practices seem to be similar to those documented by this author in his April 2002 [Domains Reregistered for Distribution of Unrelated Content: A Case Study of "Tina's Free Live Webcam"](#).

A review of the current registrants of domains previously held by NicGod suggests that certain registrants, among them the major American firms of Hewlett-Packard and AOL, are coming to hold certain domains held by NicGod as recently as March of 2002. These firms may be purchasing the domains at issue from NicGod or may be using a UDRP or similar challenge to obtain the domains.

Update: This author attempted to contact NicGod at one of the phone numbers provided in WHOIS contact records. In a return call of four days later, the author learned that a randomly-selected NicGod-registered domain was available for \$1200 (asking price) and could be transferred within 24 hours. The NicGod representative suggested payment via an escrow company, Paypal, or Afternic, noting that Afternic would charge a \$100+ fee that he thought to be excessive. The NicGod representative responded to complaints about the proposed fee by reporting the randomly-selected domain's popularity in search engines Lycos, Hotbot, and Altavista and further noting that the domain received, in his experience, 200 or more "type-in" requests per day. When asked about the minimum price he had ever accepted for a domain name ("to avoid a loss" as he put it), the representative said \$550 was his minimum, and when asked about his identity, he said he had "no secrets" and that his name was in fact Allen Ginsberg, notwithstanding that this is also (but, he seemed to suggest, only coincidentally) the name of a famous poet. The NicGod representative spoke fluent English in a heavy accent that this author found consistent with the hypothesis of Eastern European national origin. Caller ID was blocked on his incoming call. (May 15, 2002)

Update: I have added nearly 1500 additional domains currently or recently registered to NicGod, increasing the count of domains documented here from 1278 to 2754. (June 3, 2002)

WHOIS Errors and "Tricks": NicGod's Methods for Keeping Its Identity Secret

A review of NicGod registration practices shows a variety of techniques that seem to be used to keep secret the identity, location, and contact information of the NicGod staff.

The NicGod domains are notable for their wide variety of registration methods and purported contact locations. NicGod's domains use a total of eleven distinct registrars; leading registrars are Bulkregister (1294 domains), Dotster (379), The Registry at Info Avenue (285), eNom (154), Namescout (113), and iHoldings / dotRegistrar (62). Furthermore, NicGod provides at least nine distinct countries for registration of its various domain names, including Armenia, Bulgaria, Canada, Estonia, Germany, Hong Kong, the Netherlands, Russia, the Ukraine, and

the United States. A series of investigations has shown various of these addresses to be invalid. ([International Herald Tribune](#), [Detroit News Online](#) / [Bloomberg News](#), [Radio Free Europe](#)).

In addition to using a large number of invalid addresses for the registration of its domains, in many instances NicGod seems to enter the names of one or more well-known individuals as the purported registrant of its domains. For example, some 425 NicGod domains purport to be registered by [Allen Ginsberg](#), also the name of a deceased American poet. For other domain registrations, NicGod uses a variety of company names -- including "Domain ForSale," "Grafikal Kompilations," "Merkus, Matching," "Triple Zero Networks," and "Ugol Hostmaster." An [OECD report](#) further alleges that in some instances NicGod uses or previously used as the registrant name for one domain the prior registrant's name from another domain -- causing substantial confusion as to who is responsible for NicGod's registrations.

Many of the domains registered by NicGod offer a telephone and fax contact in the United States. The specified phone number is a voice mail box in the 309 area code assigned to Bloomington, Illinois. [Documentation gathered by the OECD](#) suggests that NicGod may purchase this service from an Illinois voice mail firm; in this case, NicGod itself may nonetheless have no actual presence in Illinois.

[Data collected by Patrick Jones of UDRPlaw.net](#) suggests that NicGod has faced at least 27 challenges under the [Uniform Domain-Name Dispute Resolution Policy](#) (UDRP) but has in every instance failed to respond to complaints. It is possible that staff of NicGod would prefer to forfeit their domains under the UDRP, rather than reveal their identity by responding to a UDRP complaint; alternatively, staff of NicGod may not receive UDRP complaints precisely as a result of the invalid contact data provided by NicGod to its registrars.

Of course, even NicGod's methods may ultimately prove inadequate for keeping secret its identity. Most or all NicGod domains are hosted at [dslextrême.com](#), an ISP in Canoga Park, California; it is possible that this firm knows the true identity and location of NicGod, information that it might have obtained in the course of billing or customer support. Alternatively, any of NicGod's registrars might know the firm's identity location from similar interactions. It is possible that any or all of these firms might disclose known information on the basis of a subpoena or other request. A [Detroit News Online / Bloomberg News article](#) suggests that the individual behind "NicGod Productions" may be Emil Lazarian, an 18-year-old Armenian exchange student.

Specific Domain Registrations with Invalid Contact Data

In recent testing and archiving, I have prepared a listing of a total of 2754 distinct domains that are (or recently were) registered to (or by) NicGod, and that likely offer (or recently offered) invalid contact data.

For each domain, I have attempted to obtain a variety of information including:

- Current title of default web page (as of May-June 2002)
- Date of domain registration by current registrant, when available from registrar; name of current registrar

- Prior page title, when available from archive.org (as of approximately January 1, 2000)
- Prior META DESCRIPTION and KEYWORDS tags, when available from archive.org (as of approximately January 1, 2000)
- Current Yahoo category, when available from Yahoo (as of May 2002)
- Other pages referencing or linking to domain, when available from Google (with counts as of May-June 2002)
- The number of times the domain's default web page was accessed by [Alexa](#) users between December 2001 and May 2002, with rank data when available
- The domain's registrant and administrative contact of record (as of May 2002)
- Access to page archives, when available from archive.org

The results of this data collection effort are freely and publicly available. Due to the large size of the listing of results, the listing is provided in sections by first letter of domain name:

[A B C D E F G H I J K L M N O P Q R S T U V W X Y Z numbers](#)

Summary Statistics

Of the 2754 distinct domains registered to NicGod, 2027 (73.6%) currently point to listings of links with pop-up advertising and possible click-through sponsorship. Of the remaining 166 domains, at least some have been transferred to other registrants (among them AOL and HP), and at least 43 offer sexually-explicit images.

According to current testing in Google, 2170 of NicGod's domains (78.8%) are mentioned in one or more web pages (as via a link or a textual reference to the domain name).

Yahoo continues to classify 246 of NicGod's domains (8.9%) into its hierarchical directory categories. In a casual inspection, none of these categories seems to properly characterize the content available from NicGod.

Archive.org reports that at least 2027 (73.6%) of NicGod's domains previously contained a title suggesting the availability of other content.

NicGod uses at least eleven different registrars (primarily Dotster, Bulkregister, and Namescout) and uses multiple registration addresses in at least nine distinct countries. Contact information in some registrations invokes the names of well-known individuals who are deceased as well as unaffiliated with NicGod.

Of NicGod's domains, [Alexa](#) toolbar logs reflect that the most popular were ITLIBRARY.COM (previously a resource about information technology) and ASCGAMES.COM (a computer game developer site). In the past six months, these sites received 131788 and 59361 accesses, respectively, from users of the Alexa toolbar -- making them, at least among Alexa users, the 3161th and 6877th most popular sites on the web. A total of 75 of NicGod's domains received more than 100 requests from Alexa users in the past six months -- suggesting that many of NicGod's domains were and remain relatively popular.

Possible Conclusions

While the data linked above is but a single case study of what is known to be a more widespread phenomenon, it is nonetheless possible to draw certain conclusions on the basis of work completed to date. Possible conclusions include the following:

- There exist substantial numbers of registrations with intentionally-invalid WHOIS contact information, and at least some registrants take significant deliberate steps to obfuscate their true identities and locations.
- Of registrants providing intentionally-invalid WHOIS contact information, at least some register and hold large number of domains.
- The problems with DNS are interrelated in the sense that those who register large numbers of domains with invalid WHOIS contact information may also engage in other activities of concern. For example, registrants offering invalid WHOIS contact information may tend to be the same registrants who reregister large numbers of domains for the distribution of unrelated and/or sexually-explicit materials, or who offer sexually-explicit material on domain names that do not immediately suggest the availability of such materials.
- Links and other online references continue to point to domain names even many months after those domains have come to host content inconsistent with the suggestion of the linking or referencing pages. This phenomenon holds both for relatively small linking entities (i.e. ordinary web pages) as well as large firms (such as Yahoo).
- The domains registered by NicGod are not "forgotten" or "unimportant." Indeed, many of these domains receive or previously received many thousands, if not millions, of accesses per year.

Future Work, Discussion, and Policy Implications

This work has focused on only several hundred registrations by a particular single firm. While that firm is in some circles notorious for the invalid data it enters into the WHOIS database, it would be desirable to collect additional data so as to better understand the scope of the problem. Unfortunately, large-scale analysis is difficult because it is in many instances time-consuming, difficult, and costly to determine whether or not a given contact is in fact invalid. Future work will seek to develop additional automated methods for verifying telephone numbers, for cross-checking telephone numbers with street addresses, and for otherwise recognizing suspect trends in WHOIS data. To this end, the author welcomes submission of additional examples of domains with intentionally-invalid contact information; send such submissions [to the author](#).

While a full policy analysis is beyond the scope of the current project, available data suggests that existing work by registrars and ICANN has been unsuccessful in assuring the accuracy of WHOIS data. Instead, systematic errors have remained over time, and known-abusers have continued to register at least hundreds of domains without providing valid contact information.

In this context, ICANN's recent [Registrar Advisory Concerning Whois Data Accuracy](#) seems arguably too limited to fully and efficiently address the entire problem at hand. Instead, when a given domain is found to contain invalid contact information, and when this contact information is found to be intentionally invalid, a registrar might consider canceling *all* of that registrant's

domains rather than only a particular single domain. (To reduce the risk of error, the registrar would of course first use all available methods to attempt to contact the registrant. Furthermore, the domains at issue would initially be placed into some sort of "hold" status wherein they do not function on the Internet yet, for a limited time, can be returned only to the prior registrant but not to any other interested party.)

[John Berryhill](#) points out that improvements in the accuracy of the WHOIS database may have a dual effect -- first, as expected, to increase the ability of interested parties to learn the identity of the registrant of a given domain; second, to use that registrant's contact information to induce the registrant to transfer the domain to some other registrar or to otherwise defraud the registrant. ([More information about domain name scams from the FTC.](#))

Some registrants may prefer to keep their contact information confidential. ICANN's Registrar Accreditation Agreement anticipates this possibility and therefore allows registrars to hold registrants' valid contact information in trust, while publishing in WHOIS only a placeholder address. Certain third-party firms provide a similar service. Note, however, that these intermediary services are separate and distinct from the large-scale intentional entry of invalid contact information that is the subject of this document's discussion and of which NicGod is an example.

Motivation

The purpose of this work is primarily academic -- to document the activity at issue for the benefit of those who seek to make policy decisions on related matters. In the context of ICANN's recent [Registrar Advisory Concerning Whois Data Accuracy](#) as well as associated Congressional [hearings](#), the availability of this data and analysis is intended to be helpful to policy-makers and other interested parties.

This page is made available to inform discussion about the registration of Internet domain names. The data contained here is not intended for use for other purposes, and it should not be used for other purposes without first contacting the author.

In order to confirm the results of my testing and to attempt to obtain certain other information, I sent an email inquiry to various of the contacts listed in WHOIS records of domains registered by NicGod. I have to date received no reply to the questions posed. Comments from NicGod staff remain welcome, as are comments from others interested; with the permission of the author, comments may be posted or linked from this page as appropriate.

[Ben Edelman](#)

Last Updated: June 2, 2002 - [Notify me of major updates and related work.](#)

This page is hosted on a server operated by the [Berkman Center for Internet & Society](#) at [Harvard Law School](#), using space made available to me in my capacity as a Berkman Center affiliate for academic and other scholarly work. The work is my own, and the Berkman Center does not express a position on its contents.

8/29/2003

Large-Scale Registration of Domains with Typographical Errors

Benjamin Edelman - Berkman Center for Internet & Society - Harvard Law School

[[Background](#) - [Specific Registered Domains](#) - [Analysis](#) - [Conclusions](#) - [Support This Work](#)]

Abstract

The author reports more than eight thousand domains that consist of minor variations on the addresses of well-known web sites, reflecting typographical errors often made by Internet users manually typing these addresses into their web browsers. Although the majority of these domain names are variations of sites frequently used by children, and although their domain names do not suggest the presence of sexually-explicit content, more than 90% offer extensive sexually-explicit content. In addition, these domains are presented in a way that temporarily disables a browser's Back and Exit commands, preventing users from exiting easily. Most or all of the domains are registered to an individual previously enjoined by the FTC from operating domains that are typographic variations on famous names, and these domains remain operational subsequent to an injunction ordering their suspension.

Related Projects

- [Domains Reregistered for Distribution of Unrelated Content: A Case Study of Tina's Free Live Webcam](#)
- [Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale"](#)
- [Other work by the author](#)

Background

This document investigates the registration of domain names that are minor typographical variations on well-known names in which the registrant lacks any legal right — a practice sometimes called "typosquatting." The registrations reported here are also notable in at least three additional respects: First, many of these registrations feature invalid WHOIS data, failing to correctly report the name and contact information of a domain's registrant. (This is generally as described in the author's June 2002 [Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale"](#).) Second, many unexpectedly provide sexually-explicit content, even though their domain names do not suggest the availability of such content. (This is generally as described in the author's May 2002 [Domains Reregistered for Distribution of Unrelated Content: A Case Study of Tina's Free Live Webcam](#).) Finally, many make it difficult for a user to exit the site, blocking the ordinary operation of a web browser's Back and Close commands.

Of the domains reported here, most or all are registrations by John Zuccarini, doing business under multiple names including Mars Attack, Music Wave, Party Night Inc, Phayze 1 Phayze 2, and RaveClub Berlin. These many names (and their associated invalid WHOIS data) make it difficult to determine whether any given domain is in fact registered by Zuccarini, or whether domains were instead registered by others, but the author has endeavored to report only domains registered by Zuccarini.

Mr. Zuccarini's domain registrations have produced a series of legal challenges. According to a recent [FTC press release](#), Zuccarini has faced seven federal court cases (including cases under the federal Anticybersquatting Consumer Protection Act, or ACPA) and 56 UDRP arbitration proceedings (including UDRP challenges from Abercrombie & Fitch, American Airlines, the Backstreet Boys, Encyclopaedia Britannica, Hewlett Packard, Neiman-Marcus, Target, Voicestream, and Yahoo). (See Google listings of decisions from [WIPO](#) and the [National Arbitration Forum](#).) In October 2001, the [FTC](#) brought suit against Zuccarini, challenging what the FTC called his "copycat" web addresses as well as his "mousetrap" techniques of preventing web users from exiting his sites. (The [FTC's](#) site provides their [complaint](#), [temporary restraining order](#), and [preliminary injunction](#).) In May 2002, the FTC won a [permanent injunction](#) against Zuccarini (see the FTC's [May 2002 update](#)), barring Zuccarini from registering domains that are misspellings or other variations on third-party domain names, and further prohibiting him from obstructing a visitor's exit from a site. Nonetheless, eight months after the injunction was issued, the author's research demonstrates that the enjoined behavior continues: More than five thousand domains remain registered to Zuccarini or the company names he previously used; the overwhelming majority are typographical variations on well-known trademarks, popular phrases, and personal names. Most of Zuccarini's domains still

provide traps to delay or confuse a user's attempts to exit, and most still provide extensive sexually explicit content. The remainder of this document details these findings and their implications.

Specific Registered Domains

The author has located more than 8,800 domains registered, according to their WHOIS data, to John Zuccarini or his various company names (as identified by the FTC). This quantity is generally consistent with prior [FTC reports](#) of "more than 5,500" domains registered by Zuccarini; some domains may have expired in the interim, while others may have been added, and the FTC may not have been aware of all of Zuccarini's registrations.

The links below provide an alphabetical listing of the domains registered to Zuccarini. Each domain's entry includes selected additional information about it, including the domain's registrar, partial WHOIS data, and a categorization of the content posted on the domain's web site or post-redirection target.

[A B C D E F G H I J K L M N O P Q R S T U V W X Y Z numbers](#)

Due to the large number of domains registered by Zuccarini, the author has selected a sample of domains that reflect typographical errors on some of the most popular domain names and on domain names often used by children.

[Highlights](#)

Since the majority of Zuccarini's domain registrations are variations on other domain names, this site provides a system for users to help characterize the connections between Zuccarini's registrations and the domains he targeted with typographical variations. For example, the domain name "woldmap.com" (sic) is a variation on the name "worldmap.com." To submit such a variation to the database on his site, follow the links marked "If this domain name contains a typo, suggest the name it derives from." The author will review all submissions and will post frequent updates to this site. In the future, the author may also post summary statistics of these results, and the author hopes to send messages to the registrants of the original domains to alert them to Zuccarini's variations on their domain names.

Reporting includes only Zuccarini names listed in .COM, .NET, and .ORG zone files of January 23, 2003 and March 21, 2003. Domains omitted from these zone files are omitted from the author's data collection systems and from his subsequent analysis. Pending UDRP decisions are one frequent cause of omission from zone files and therefore from the author's reporting; domains with pending UDRP decisions are omitted from zone files due to their *REGISTRAR-HOLD* status.

Analysis and Summary Statistics

Invalid WHOIS Data and Obfuscation. As described by the FTC, Zuccarini's use of multiple identities makes it difficult to confirm that the domains at issue are indeed his. Of the domains reported here, registrations are made in the name of John Zuccarini, Mars Attack, Music Wave, Party Night Inc, Phayze 1 Phayze 2, and RaveClub Berlin. Registrations are made from countries including the United States, the Bahamas, Burkina Faso, France, the Netherlands, and Switzerland. It is possible -- indeed, highly likely -- that Zuccarini holds numerous additional domains beyond those reported above. The author selected the domains reported here on the basis of multiple factors linking them to Zuccarini; relevant factors include WHOIS data, registrars used, DNS and web site configuration, and web content.

Registrars Used. Of Zuccarini's registrations reported here, most used registrars [Joker.com](#) (4,583 domains, 54.7% of those reported here) and [Key-Systems GmbH](#) (3,289 domains, 37.3%). As discussed below, these two registrars are both based in Germany, producing potential jurisdictional complications in the resolution of disputes regarding Zuccarini's registrations. Zuccarini also registered domains with [Register.com](#) (66) and [Network Solutions](#) (49). No other registrar registered more than ten of Zuccarini's domains.

Content Provided. At least 7,904 of Zuccarini's domains (90.0%) provide redirection to the site amateurvideos.nl, a sexually-explicit site that uses "mousetrapping" to prevent direct exit via a browser's Back button or via other ordinary browser commands. Provision of sexually-explicit content may be profitable to Zuccarini via at least two independent avenues: First, the FTC's complaint suggests that Zuccarini may have profited in part from affiliate fees paid to him when visitors make purchases from the sexually-explicit sites that are the targets of his redirects. Second, to the extent that Zuccarini anticipates selling domains to the registrants who hold the "real" sites on which Zuccarini's domains are variations, providing sexually-explicit content may increase the registrants' willingness to pay. (See related discussion in "[Domains Reregistered for Distribution of Unrelated Content: A Case Study of Tina's Free Live Webcam](#).") An additional 342 of Zuccarini's domains (3.9%) forward users to sites offering digital music downloads and tools; the domains that redirect to this content are variations on the names of products used to obtain digital music files.

Reconfiguration of Zuccarini Domains: Notwithstanding the court's injunction requiring the termination of Zuccarini's use of these domains, Zuccarini seems to maintain the ability to access and reconfigure his domain names. According to [Verisign Registry WHOIS](#) data, 7,547 of Zuccarini's domains (85.7% of those reported here) have had a configuration change since April 9, 2002, when the injunction was issued. Such changes are typically made only by a domain's registrant.

Domain Creation and Expiration Dates: According to data in WHOIS, the overwhelming majority of Zuccarini's domains were registered between August 1999 and March 2002. (However, fifteen domains were registered prior to August 1999. Eighteen domains were registered between April 2002 and August 2002, though none were registered since that time.) Most of Zuccarini's domains are slated to expire in 2003, but some will expire in January 2004, and a handful show expiration dates as late as May 2006.

Interaction of Typographical Variations with Trademarks: Mr. Zuccarini's registrations consist of variations both on trademarks and on generic terms. To the extent that Zuccarini's registrations are variations on trademarks (e.g. verizonwierless.com), the UDRP applies under its "confusingly similar" standard ([section 4.a.i](#)). To the extent that Zuccarini's registrations are variations on generic domains (e.g. woldnap.com), the UDRP does not apply, for the UDRP would not protect those generic domains on which certain of Zuccarini's domains are variations. Of course, there may as yet be no consensus (within the ICANN policy framework, or under governing national law) as to the rights of the registrant of a generic domain in typographical variations on that generic domain.

Conclusions

The continued operation of Zuccarini's domains suggests a possible failure of the various laws and policies to date brought to bear on his activities. UDRP challenges have proven effective for those domains targeted by specific UDRP actions. However, the UDRP entails a cost of several thousand dollars per domain (including both filing costs and attorneys fees), so UDRP expenses might well reach to the millions of millions of dollars due to the number of domains registered by Zuccarini. In this context, the FTC's en masse approach seems more likely to be effective. However, the FTC's action and the court's subsequent injunction seem to have failed to fully prevent the harm at issue, for Zuccarini continues to hold domains that seem to violate the court's injunction. Nonetheless, Zuccarini's current "mousetrapping" is somewhat less effective than his prior implementation, yielding fewer popup windows when a user attempts to close a Zuccarini site, suggesting that the FTC's injunction may have yielded improvement in this regard.

Jurisdictional issues may make the situation particularly difficult to resolve: Zuccarini has reportedly moved to the Bahamas ([cite](#)), from which extradition would likely be required to enforce a judgment of an American court. In addition, an American court may lack any way to order foreign registrars to take action, and Zuccarini's primary registrars ([Joker.com](#) and [Key-Systems GmbH](#)) are based in Germany. To improve compliance in the future, an American court might order specific actions by registrars and might send copies of its order directly to registrars (rather than relying on the defendant to do so, as explained in the court's [permanent injunction](#)). Even so, non-US registrars may refuse to comply. Concerned parties might seek to convince ICANN to address the situation -- perhaps by requiring registrars, under the terms of their [accreditation agreements](#), to comply with orders of American courts. (The current [Registrar Accreditation Agreement](#) requires, in [section 3.7.7.10](#), only that a registrar abide by orders from courts in the registrar's jurisdiction and in the jurisdiction of the registrant -- the latter provision effectively unusable in the face of heterogeneous and invalid WHOIS data.) Of course, such an

approach would raise jurisdictional problems of its own: American registrars might protest a symmetrical duty that required their submission to orders from non-US courts. Alternatively, the UDRP might be modified to better address the possibility of large-scale offenders with hundreds or thousands of domains -- avoiding the jurisdictional problems inherent in suits in national courts, but expanding the UDRP's evidentiary and procedural scope to accommodate the increased complexity of larger cases. For now, the jurisdictional provisions of existing policies allow Zuccarini to contest UDRP decisions against him (under [UDRP rule 4.k](#)) via suits in German courts; Zuccarini has contested rulings against him in claims brought by Toyota, Vanguard, and Classmates Online Inc., as documented in links 67-69 of [UDRP Law.net's appeals page](#).

Meanwhile, pending a widening of jurisdiction over registrars or of the UDRP, courts that seek to enjoin behavior like Zuccarini's may take certain actions to increase the likelihood of registrar compliance. Whenever possible, courts could list all the specific domains to be transferred, cancelled, or put on hold -- giving registrars complete clarity as to the requested action, rather than demanding that they determine which domains are held by a particular offender. With the help of plaintiffs' counsel and experts if needed, along with the power of discovery, a court might be better able to identify the offender's domains than would the registrars at issue. When invalid WHOIS data makes it particularly difficult to identify the offender's domains, bringing this process under the control of the court relieves the burden on registrars who, in the face of difficult decisions and uncertain obligations, might otherwise choose to do nothing. In addition, anticipating registrars' fear of ambiguity in the wording of an injunction, a court might list prohibited activities with ever-greater specificity. The Zuccarini injunction shows room for improvement in this regard: It prohibits "operating, publishing, or disseminating web sites or pages with domain names that are misspellings of other domain names" (clause L.1.) -- a restriction that might be alleged to leave open the question of what constitutes a "misspelling" and that might thereby discourage some registrars from taking action.

The FTC [advises](#) that individuals who believe they have been victimized by Mr. Zuccarini can register their complaints via a toll-free telephone call to 1-877-FTC-HELP (1-877-382-4357).

Support This Work

Partial support for this project was provided by the [Berkman Center for Internet & Society at Harvard Law School](#). The author seeks additional financial support to continue this and related projects. Please [contact the author](#) with suggestions.

Last Updated: April 6, 2003 - [Sign up for notification of major updates and related work](#).
An earlier version of this article was posted in January 2003, offering an initial listing of approximately 5,500 domains registered by Zuccarini.

Survey of Usage of the .US TLD

[Introduction - Methodology & Results - Conclusions & Future Work]

Abstract: Recent policy changes allow registrations in .US with few restrictions. The author collects data about all known .US registrations, analyzing their registration patterns and usage. Certain registrants are found to register more than 2,000 domains each; these registrants may be gathering domains for commercial applications requiring many domains or for future sale, and large registrants (with ten or more .US domains) jointly hold a total of 46.4% of .US registrations to date. Non-Americans are found to register 7.0% of domains, and some of these registrations may violate .US registration restrictions that require nexus in the United States. The overwhelming majority of .US registrations as yet provide no original web content; working .US web sites are found to be clustered with certain registrars, while certain other registrars tend to register domains that offer no web content and domains offered for resale.

Introduction

In 1985, Jon Postel created a series of top-level domains for use by interested countries; among these so-called country-code top level domains ("ccTLDs") domain was .US, bearing the two-letter country code ordinarily associated with the United States. For more than a decade thereafter, .US registrations were generally permitted only within a strict hierarchy reflecting both geographic and organizational categorizations (i.e. www.k12.wa.us for the public schools in Washington State). However, the National Telecommunications and Information Administration of the US Department of Commerce in 1998 began a consultation process, to consider a liberalization of the .US registration hierarchy, and in the spring of 2002 .US was opened for second-level registrations (i.e. cars.us) via newly-selected registry operator Neustar and competitive registrars.

Four months after the opening of .US to public registration, the author seeks to investigate usage to date of the .US space. Such investigations in part follow the model of the author's previous studies of domain names, quantifying top registrants, registrar market shares, warehousing, defensive registrations, and cybersquatting. Analysis further considers .US domains that may not comply with .US registration restrictions.

Methodology & Results

To analyze domain registrations and use, the author began with a full listing of all registered .US domain names. Many TLDs provide such a listing upon request, via a so-called "zone transfer" often accompanied by a license agreement; however, Neustar told the author that zone file is currently available only to .US registrars but not to the general public (email communications of May 21, 2002 and August 12, 2002). The author sincerely thanks a .US registrar, who prefers to remain anonymous, for providing the zone file so central to subsequent analysis.

The author used automated systems to collect data about each registered .US domain. From publicly-available WHOIS data, the author collected registrant name and organization, registrar, and date of registration, as well as the country of registrant and of administrative, billing, and technical contacts. The author further collected the title of each domain's default web page (when available).

Analysis uses the .US zone file of August 13, 2002, which includes a total of 307,788 distinct .US domains.

Results include the following five sections:

[Registration Patterns of Top .US Registrants](#)
[Registrations by Non-US Registrants](#)
[Rate of Registration](#)
[Registrar Market Share](#)
[Domain Usage & Registrar Specializations](#)

Registration Patterns of Top .US Registrants

Certain registrants were found to register a large number of .US names. For example, Bryon Uding of the American Spirit registered 2,494 .US domains, Bradley Norrish of Internet Registrations Worldwide registered 1,746, and Sanda Yackolow of Marblehead Consulting registered 1,500. The tables linked below summarize and detail .US registrations by registrants with ten or more .US domains.

[.US Registrations by Top Registrants](#)
[.US Registrations by Top Registrants, with domain listings](#)
 Page [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#)

Note that some "top registrant" listings reflect registrations in the name of a registrar. The author contacted representatives of certain registrars and was in most instances told that these registrations will in due course be modified to reflect registration by registrars' existing customers.

Inspection of the registrations of top registrants shows five notable categories of .US domains. The first three categories listed below are specific to the "us" string specifically, while the final two are consistent with open TLDs generally.

- *Geographic locations.* Some domains bear city names (for example, [albany-ny.us](#) and 929 other names registered by Gagan Patnaik), while others include both place names and product names ([bronxrealestate.us](#) and many of the 554 other names registered by Max Rinaldi).
- *Other US-specific content,* including content that is explicitly patriotic or otherwise related to the United States.
- *Other usages of "us."* For example, many domains use the string "us" to signify not "United States" but rather the first person plural objective pronoun. Examples include many of the 2494 registrations by Bryon Uding, such as [a-good-time-with.us](#) and [bargains-for.us](#).
- *Defensive registrations.* Trademark holders have submitted a variety of registrations to prevent use of their marks by others. For example, Johnson & Johnson registered 783 .US domains including product names ([childrenstylenoflu.us](#)) and generics ([allaboutkneesurgery.us](#)); consistent with the author's prior investigation of defensive registrations, these domains do not provide web pages. Amazon took a different approach with the registration of sixteen names seemingly intended to help users who make typos or to prevent others from "typosquatting" on Amazon's marks; Amazon's .US registrations include [aamazon.us](#), [amaozn.us](#), and [amazon.us](#), and these sites all redirect to Amazon's ordinary web site at [amazon.com](#). Defensive registrations in .US include registrations by non-American firms such as Unilever (99 .US domains registered) and Emirates Airline (24).
- *General registrations of arbitrary strings.* As expected in an open TLD, .US domains include a large body of content of general registrations. Among top registrants, notable examples include most or all three-letter .us domains ([aaa.us](#) and so forth, including the overwhelming majority of Bradley Norrish's 1746 registrations), generic business names ([bookstore.us](#) and many others of Richard Leeds' 1,333 registrations), and sexually-explicit content ([all-animalsex.us](#) and 833 other domains by Silver Back Corp).

Registrations by Non-US Registrants

Certain .US domains were found to provide (in their WHOIS registrant and contact data) addresses outside the US. Under the [.US Nexus Requirements](#) (PDF), .US domains may be registered only by 1) US citizens or residents, 2) US entities or organizations, and 3) foreign entities or organizations with a *bona fide* presence in the US. To determine whether a foreign entity has such a presence, registration requirements specify consideration both of a registrant's ordinary lawful activities within the United States and of a registrant's offices or other facilities in the US.

The author knows of no automated means of confirming that a registrant in fact complies with nexus requirements; indeed, Neustar's Nexus Requirements document contemplates only occasional scans and spot checks. However, when a non-US registrant holds many .US names, the registrant may be particularly likely not to comply with stated nexus requirements; a non-US registrant holding dozens or hundreds of .US names, each pointing to an "under construction" site or an error message, might be thought more likely to be a domain warehouse or reseller than a foreign entity with a bona fide presence in the US. Accordingly, the author below reports those registrants who have registered 5 or more .US domains that each provide addresses outside the US for registrant address and for administrative, billing, and technical contacts. Of course, many of these registrations no doubt comply with Nexus Requirements, but at least some may reflect registration by a non-US individual or by a non-US organization without the required US nexus.

.US Registrations by Non-US Registrants

Of .US registrants with all contacts outside the US, some registrants registered many .US domains. Silver Back Corp (of Antigua and Barbuda) registered 834 domains including all-animalsex.us, alyssa-milano-gallery.us, alyssa-milano-naked.us, and alyssa-milano-nude.us; Global DNS Services (of the Netherlands) registered 474 domains including 11b.us, aanbieding.us, aanbiedingen.us, and adult-toy.us; B.Stone of the Netherlands registered 226 including afterparty.us, ahold.us, americangigolo.us, and americanpornstar.us. A total of 613 distinct registrants registered 5 or more domains with all contacts outside the US, and a total of 21,639 domains were registered with all contacts outside the US (7.0% of all .US registrations to date).

As detailed in the .US WHOIS FAQ, each .US domain includes a designation of its nexus code. Possible codes include C11 (US citizen), C12 (permanent resident of US), C21 (US organization), C31 (foreign entity or organization with bona fide US presence, regularly engaging in lawful activities in the US), and C32 (office or other facility in the US). As among .US registrations with all contacts outside the US, the table below reports the number of registrants providing each of these nexus codes:

	Number of .US Registrations	Proportion of .US Registrations
	(among .US registrations with all contacts outside the US)	
US Citizen	3392	15.6%
Permanent Resident of US	751	3.5%
US Organization	1373	6.3%
Foreign Entity or Organization with Bona Fide US Presence, Regularly Engaging in Lawful Activities in US	12766	58.7%
Office or Other Facility in the US	2848	13.1%
No nexus data available in WHOIS	609	2.8%

Impermissible .US registrations (by registrants without the required nexus) may tend to take place within certain purported nexus codes. However, research to date has not identified nexus codes disproportionately used for this purpose.

Rate of Registration

WHOIS "Domain Registration Date" data provides information about the date of registration of each registered .US domain.

.US Registrations Per Day - chart and table

This data reflects that more than 56% of .US name were registered on or before April 30, 2002 -- in the .US

sunrise process. Since that time, approximately 1,000 .US domains have been added per day; this rate has remained roughly constant since June 1, 2002. Clear weekly trends reflect fewer registrations on weekends than on weekdays.

With approximately 308,000 domains registered through August 13, 2002 and a growth rate of 1,000 domains per week, extrapolation suggests a total of approximately 332,000 domains on January 1, 2003.

Registrar Market Share

Interested registrants obtain .US names through [accredited .US registrars](#). The chart and table linked below summarize registrar market share to date.

[.US Registrar Market Share - chart and table](#)

This data reflects that leading .US registrars are Go Daddy (55,687 .US names, 18.09% of registrations to date), Register.com (42,645, 13.86%), Verisign (38,578, 12.54%), Enom (27,437, 8.92%), and Directnic (16,740, 5.44%). Together, these five registrars sponsor 58.84% of .US registrations, while a total of 65 other registrars sponsor the remaining 126,661 .US domains.

Among the twenty largest .US registrars, 12 registered between 40% and 80% of their .US names during the .US sunrise. Certain other registrars did not participate in the sunrise; Wild West Domains registered its first domain on July 16, and Stargate Communications registered its first on July 27. Other registrars have registered only minimal names since the sunrise; such registrars include "Official US Domains" (6,245 sunrise registrations and 494 subsequently), Encirca (5,008 and 940), and Namescout (5,537 and 388). Additional details are available in the chart and table linked above.

Domain Usage & Registrar Specializations

The author attempted to obtain the default web page from each registered .US domain name, and when those pages were available, the author categorized available content into the groupings described below. Review and grouping of HTML page titles provided automated categorizations of the majority of tested web sites, while manual review was used for certain additional domains that could not be classified based on their ambiguous or omitted HTML page title.

	<i>Proportion of all .US domains</i>
Fails to provide a valid HTTP response ("cannot connect to server")	30.2%
HTML body is blank, provides a redirect, or includes "under construction," "coming soon," or similar	50.6%
HTML title or body contains an offer of sale	2.8%
Error message	1.1%
Uncategorized (includes domains with actual content)	15.3%

The large number of .US domains without default web pages, with blank pages, and with "under construction" or similar pages is consistent with the author's prior study of other top-level domains including [.BIZ](#) and the open country-code top-level domains of [.CC](#), [.TV](#), and [.WS](#).

With knowledge of each .US domain's registrar, the author tabulated domain usage by registrar. As detailed in the table linked below, registrars vary greatly in their customers' usage of .US domains. Large .US registrars with relatively high estimated rates of provision of web content include Tucows (29.6%), Bulkregister (24.9%), Enom (23.5%), Go Daddy (17.9%), and Verisign (17.1%). Large registrars with substantially less frequent provision of

web content include Itsyourdomain (5.0%), Dotregistrar (6.2%), and Directnic (7.7%). Note, however, that certain large registrants can sway these estimates dramatically; for example, a single Bulkregister registrant provides substantially the same content on all of its 1,333 .US domains, but since these domains do provide actual web content, they count towards registrar Bulkregister's total and increase its "actual web content" proportion by 11.5%.

Registrants of certain registrars chose "under construction" pages for the overwhelming majority of their domains; for example, fully 83.1% of domains by registrar "Official US Domains" provided "construction" pages or were blank or redirects. However, registrations by certain other registrars disproportionately tended not to provide valid HTTP responses, perhaps because these registrars do not provide "under construction" pages or because their customers prefer not to use such pages; such registrars include R&K Global Business Services (87.3% of registered domains fail to provide a valid HTTP response), Encirca (88.5%), and Emarkmonitor (96.0%).

Domains with offers of sale tended to be clustered with registrars Domain Discover (42.5% of registered domains included an offer of sale on their default web pages), Directnic (11.0%), and CORE (18.9%). This result also primarily reflects clumping of registrants -- that these registrars each have one or several large registrants with many domains offered for sale.

Domain Usage by Registrar

Conclusions & Future Work

According to Neustar's Director of Policy and Business Development, the .US registry is and ought to be "a national public resource" (cfile, PDF). In this context, evaluation of .US's registrations to date may properly examine registration trends with an especially detailed level of scrutiny. Registrations like those of Silver Back Corp of Antigua and Barbuda (834 .US domains including all-animalsex.us and alyssa-milano-naked.us) may come into question for disputed compliance with .US nexus requirements. In addition, while the resale of domains is permissible under .US registration rules, those who register hundreds or thousands of names for the purpose of resale may also find their actions controversial.

The author knows of no proactive enforcement of .US registration restrictions, and it is therefore perhaps not surprising to find many thousands of domains that may be inconsistent with registration restrictions. Consistent with the author's prior investigations of .NAME and .BIZ, compliance with stated registration restrictions seems to require an active and proactive enforcement mechanism; merely demanding that registrants certify compliance with stated rules may not suffice to ensure compliance. Of course, effective enforcement may be difficult and costly; indeed, it may be sufficiently difficult and costly that the Neustar registry and the US Department of Commerce on balance decide against such enforcement. Nonetheless, if current registration restrictions reflect an explicit policy decision as to proper usage of the .US TLD, current enforcement systems may be ineffective at carrying out this policy. Were the DoC and Neustar to remain committed to the current registration restrictions, they might put into place special checks for those registrants outside the US. For example, a first-time non-US .US registrant could be required to fill out a web form detailing its US activities and/or US offices or facilities, the factors considered under Neustar's current statement of Nexus Requirements.

Future work might consider the following questions:

- Change over time, including changes in registration rate, registrar market share, domain usage, and registrations by non-Americans
- Transfers, drops, and other future uses of domains currently held by large registrants
- Renewal rates, and differences in renewal rates across sponsoring registrars
- Search engine listings, and differences in listings across sponsoring registrars
- The extent to which generic .US registrations are held by the same firms that hold the corresponding domains in other TLDs
- The extent to which some large registrants have registered the trademarks of other entities

Thanks to [Prof. Eausott](#) for suggesting this project and to Tim Hewitt of [myOstrichInternet](#) for information on .US sunrise registration restrictions. Thanks also to an anonymous registrar that provided a current .US zone file.

[Ben Edelman](#)

Last Updated: September 20, 2002 - [Notify me of major updates and additions to this page.](#)

This page is hosted on a server operated by the [Berkman Center for Internet & Society](#) at [Harvard Law School](#), using space made available to me in my capacity as a Berkman Center affiliate for academic and other scholarly work. The work is my own, and the Berkman Center does not express a position on its contents.

Mr. SMITH. Mr. Farnan?

STATEMENT OF JAMES E. FARNAN, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. FARNAN. Good afternoon. I would like to thank Chairman Smith, Ranking Member Berman, and Members of the Subcommittee for the opportunity to testify today. We welcome your Subcommittee's leadership in dealing with the serious issues associated with use of the Whois database.

Cyber Division investigators use the Whois database every day. Querying of domain name registries is the first step in most cyber crime investigations. While this process identifies the entity responsible for operating an Internet site, it does not provide identifying information about users of that site.

For instance, we may receive a complaint that a website is being used to solicit personal, credit card, or financial information. Our first task is to identify the operator of that site using the Whois database. We will query the domain name registry where the target domain is registered. If the information in the registry is accurate, it will show the name, location, and contact information for the operator of that site. With this information in hand, we know where to direct the appropriate legal process to obtain additional information.

Unfortunately, there is no system for authenticating information provided to domain name registries other than to ensure that the payment mechanism, usually a credit card, is authorized at the time the domain name was purchased. In other words, a stolen credit card may be used to purchase a domain name and provide fictitious information which is never checked or verified.

In addition to law enforcement's use of domain registry information, system administrators use this information to identify sites that may be causing technical problems over the Internet or which are the source of certain abuses, such as viruses or other malicious code, and then use this information to contact the site owner to advise them of the problem.

I have two examples of cases in which Cyber Division investigators and analysts use the Whois database. In a significant intellectual property rights investigation, a site that was used to host pirated computer software had a domain name that was registered with fraudulent information. Investigators took logical steps to identify the subject who owned and operated that site, but the fraudulent information in the domain name registry substantially hampered the investigation at its critical early stages.

To obtain valid identifying information regarding the subject's location, investigators were required to implement more complex and time-consuming legal processes through a series of Internet service providers associated with Internet traffic to and from the subject website. The subject was ultimately identified and prosecuted, although the process was substantially lengthened and complicated due to the inaccuracy of information provided to the domain registry. A delay of this type in identifying subjects and locations of relevant computers could result in the loss of critical evidence or the complete failure to locate subjects.

In a second case, we received information that a particular website contained images of child pornography. Our analysts used Whois to identify the Internet Service Provider, or ISP, hosting the website. Soon, a subpoena to the ISP generated a response which provided significant leads, including web logs that generated activity in foreign countries, as well as a name for the owner/operator of the original website. There was no other identifying information on the owner/operator. Analysts searched other databases and eventually linked the subject to a previously unknown website. Using the name of the new website matched with the subject's name, and again using the Whois database, analysts were able to completely identify the subject and a geographic location.

In this example, Whois was used twice, first to generate a single subpoena to the proper ISP, and secondly, to positively identify the subject. Without the assistance of the Whois database, analysts would have had to rely on more conventional search methods which would have led to dozens of subpoenas being issued with no certainty the true subject would have ever been identified.

The use of these more conventional investigative methods is extremely time consuming and resource intensive. The Whois database greatly enhances the accuracy of the FBI's investigations as it allows analysts and agents with the ability to create—to accurately issue subpoenas, some of which may otherwise not be issued to the correct ISP.

Our interest in Whois can be summarized in one sentence. Anything that limits or restricts the availability of Whois data to law enforcement agencies will decrease its usefulness in FBI investigations, while anything that increases the accuracy and completeness of Whois data will improve timeliness and efficiency in our cases. There are other means for obtaining this information, but these can degrade efficiency and timeliness.

I thank you for your invitation to speak with you today, and on behalf of the FBI, look forward to working with you on this very important topic.

Mr. SMITH. Thank you, Mr. Farnan.

[The prepared statement of Mr. Farnan follows:]

PREPARED STATEMENT OF JAMES E. FARNAN

Good Afternoon. I would like to thank Chairman Smith, Ranking Member Berman, and members of the Subcommittee for the opportunity to testify today. We welcome your Subcommittee's leadership in dealing with the issues associated with use of the "Whois" database.

Cyber Division investigators use the Whois database almost every day. Querying of domain name registries is the first step in many cybercrime investigations. This task may help identify the entity responsible for operating an Internet web site. For instance, law enforcement may receive a complaint that a web site is being used to solicit personal credit card financial information from victims. The first task for law enforcement is to identify the operator of that site. This may be accomplished by querying the domain name registry where the target domain is registered. If the information in the registry is accurate, then it will show the name, location, and contact information for the operator of that site. With this information in hand, law enforcement knows where to direct the appropriate legal process (a subpoena, court order, or other process) if additional information is required.

Sometimes the publicly available identifying information in the Whois database is inaccurate but the non-public payment information used to purchase the domain name is valid and legitimate. In those instances, serving a subpoena on the registrar can yield the real identity of the domain owner. Unfortunately, not every domain name registrar authenticates credit card or other payment information at the

time the domain name is registered. Therefore, a suspect using a stolen credit card may be able to purchase a domain name with fictitious identifying information which is never checked or verified. Obviously we would prefer that registrars take steps to increase the reliability of the Whois database, but as I will describe in a moment, there are other tools available to law enforcement to supplement the information found in the Whois records.

Allow me to set forth the facts of a typical case in which Cyber Division investigators and analysts have used the Whois database, along with other tools, to quickly identify the targets of an investigation.

Recently, the National Center for Missing and Exploited Children (NCMEC) and the FBI received information that a particular web site contained images of child pornography. Analysts with the FBI checked the Whois database to ascertain the identity of the Internet Service Provider (ISP) hosting the web site. (Note that this information is readily available from other public sources as well.) A subpoena for information pertaining to the web site's owner/operator was soon obtained. Two weeks later, the subpoena generated a response which provided significant leads, including web logs which indicated activity in foreign countries, as well as a name for the owner/operator of the original web site. There was no other identifying information on the owner/operator.

Analysts continued to search other databases to locate any other possible businesses or locations affiliated with the subject. Eventually, a link was made between the subject and a previously unknown web site. Matching the name of the new web site against the subject's name, and again using the Whois database, analysts were able to completely identify the subject, including a geographic location.

Additionally investigators use the Whois database in investigations ranging from online fraud, threat, to computer intrusion cases. The information obtained from the Whois database is often used to generate investigative leads and is the starting point for utilizing other investigative techniques.

As the above example shows, the publicly accessible Whois database of domain name registrations can be a useful tool in law enforcement investigations. That is not to say that Whois is indispensable, however. As I've indicated, sometimes the Whois data is inaccurate, incomplete, outdated, or deliberately falsified. If the Whois data leads to a dead-end, the FBI has other tools at its disposal to obtain information concerning the identity of domain owners. Some of those tools include publicly available sources of information similar to the Whois records. For example, in addition to the Whois database covering domain name registrations, there is an entirely different set of records covering the assignment of Internet Protocol (IP) addresses. The IP address assignment records tend to be more accurate than the Whois domain name records, and in most cases they will lead us either to the domain owner's ISP or to the Web hosting company. The publicly available sources also include technical tools such as traceroute, which "traces" the electronic path to a Website, and domain name service ("DNS") lookups, which again usually reveal the ISP or the Web hosting company. Once we know the ISP or the Web hosting company, law enforcement can serve subpoenas or court orders to obtain personally identifying information for the domain name owner, or to gain leads on other useful information.

Obviously 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. In addition, although international cooperation is improving for computer crime and terrorism investigations, there is always the possibility of delay in getting responses to formal legal process whenever our investigations cross international boundaries. Whois can be useful in those cases, assuming the Whois data is accurate and complete, which it often is not.

The Justice Department is aware of efforts currently underway to enable the Internet Corporation for Assigned Names and Numbers (ICANN) to address some of the public policy issues associated with the Whois database. We are aware of these discussions and have tried to ensure that law enforcement interests are clearly understood by the participants in the ICANN process. The Justice Department has stated that it does not endorse any particular solution among those now being considered by ICANN. Anything that limits or restricts the availability of Whois data to law enforcement agencies will decrease its usefulness in FBI investigations, while anything that increases the accuracy and completeness of Whois data will improve timeliness and efficiency in our cases.

I thank you for your invitation to speak to you today and, on behalf of the FBI, I look forward to working with you on this topic.

Mr. SMITH. Mr. Kassinger?

**STATEMENT OF THEODORE W. KASSINGER, GENERAL
COUNSEL, U.S. DEPARTMENT OF COMMERCE**

Mr. KASSINGER. Mr. Chairman, Mr. Berman, Members of the Subcommittee, thank you for your warm words of welcome in your opening statements. [Laughter.]

It's true that Assistant Secretary Victory resigned a month ago and that proved to be an opportune time, but I welcome the opportunity to be here today. This is an important subject and I'm happy to represent the Department and discuss these issues with you.

In my prepared statement, I spent a fair amount of time discussing our thoughts about the MOU. I hope we'll spend more time on that in the question and answer session. That is a key task facing us.

But I wanted to take this—these brief moments here to address seriatim the six questions you posed in your letter to Secretary Evans on August 8. I thought we ought to get that on the record in simple terms, so let me briefly walk through those.

Your first question was whether—was you asked for the Department's assessment of ICANN's efforts to enforce the——

Mr. SMITH. Mr. Kassinger, of course, there was an easier way to get that letter on the record, and that would have been to respond to us before today, but we'll let that go.

Mr. KASSINGER. I take your point. You asked for an assessment of ICANN's efforts to enforce the Whois related provisions of the registrar accreditation agreements. In our judgment, ICANN's management, led by the new CEO, Mr. Twomey, understands the need for accurate and publicly available Whois data and is committed to improving the Whois system. Clearly, more work needs to be done in this area.

The two developments that you alluded to, and Mr. Berman and others—the new Whois data problem report system and the data date reminder policy—are steps in the right direction. They are not enough. I would suggest, however, that there's a lot more going on than would be suggested by some of the discussion here today. Mr. Twomey has appointed a Presidential advisory body to specifically work on these issues, and as we'll discuss—and I'll discuss in answer to your other questions, there's an awful lot of activity going on. So a lot of work needs to be done, but we think things are headed in the right direction.

Second, you asked for the steps the Department has taken to encourage ICANN registrars and registries to honor their contractual obligations. We've done a number of things in that area. First, the Department has monitored developments in the Whois arena closely since ICANN's inception and will continue to do so. The Department is particularly interested in the impact of the new complaint reporting process and the Whois update requirement on improved accuracy, but there are other things we're working on.

Second, the Department has focused its efforts in the international arena primarily through the Government Advisory Committee, the GAC, WIPO, and the International Telecommunication Union. We're active in all those fora. Most recently, the Department took a leadership role in the June 2003 education workshop hosted by ICANN that focused on Whois issues.

Third, the Department through WIPO and the GAC has actively encouraged the development and enforcement of best practices for accurate and publicly available Whois data.

Fourth, the Department has advocated the adoption of Whois type registrant contact data and dispute resolution policies for ccTLD operators in bilateral trade agreements, such as the recent trade agreements with Singapore and Chile.

And finally, we took the lead in forming a Government inter-agency working group to increase the effectiveness of our analyses and advocacy on these issues. This group includes representatives from the Department, including the PTO, the Justice Department, and the Federal Trade Commission. We're in the process of formulating a set of recommendations to be presented to the GAC at the ICANN meeting in October. So we're doing a lot.

The third question you raised was the manner in which the Department intends to address intellectual property concerns in any MOU extension. This is a conversation I'm sure we ought to have in an extended way in the Q&A session, but let me just say that we have not finalized our proposal to ICANN. This question is still on the table. How to address it is a difficult one.

Our primary focus, as indicated in the written testimony, is on matters that go to the core sustainability of ICANN. The question of how Whois data is handled would be academic if ICANN cannot survive, and we have perceived serious issues for the long term that ICANN must address in the next phase under the MOU. There is, for example, at this point, to my knowledge, no strategic plan at ICANN of where it wants to go and how it's going to get there. There is a serious question of financial resources that are essential for, among other things, to address Whois issues.

So we have identified the seven areas that were listed in my written statement. We're considering what other items should be in the MOU. We welcome your thoughts in that regard.

Fourth, you asked for the Department's opinion on whether the ccNSO structure and charter adopted by the ICANN board satisfy the MOU obligation with regard to ccTLDs. The short answer is no. We think it's a good thing. We support it. We support the effort to bring the ccTLDs into the ICANN world through that organization and the policies it may recommend, but our MOU requires actual agreements, and that is what we will look for.

Fifth—I'm sorry, Mr. Chairman, I've run out of time. If you can stand the suspense, I'll address your last two questions later.

Mr. SMITH. Okay. Thank you, Mr. Kassinger.

[The prepared statement of Mr. Kassinger follows:]

PREPARED STATEMENT OF THEODORE W. KASSINGER

Mr. Chairman,

Thank you and the members of the Subcommittee on Courts, the Internet, and Intellectual Property for this opportunity to testify on developments that affect the operation of the Internet domain name system and the enforcement of intellectual property rights in the digital environment. The Department of Commerce believes that the public domain name registrant database known as the "WHOIS" is a particularly valuable tool in enforcing intellectual property rights.

EXTENDING THE ICANN MOU

The Department continues to serve as the steward of critical elements of the domain name and number system (DNS), while pursuing the policy goal of privatizing

technical management of the DNS. The vehicle for achieving this goal is the Memorandum of Understanding (MOU) between the Department and the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is the private sector entity responsible for day-to-day management of Internet names and numbers.

The Department continues to believe that the stability and security of the DNS can best be achieved through privatization of and global participation in technical management of the system. The Department supports the ongoing work of ICANN and its efforts to engage stakeholders in its decision-making processes. The Department especially desires to see ICANN evolve into an independent, stable, and sustainable organization that is well-equipped to weather a future crisis. We are encouraged that ICANN has been making progress toward this end.

Last year, the Department and ICANN agreed to renew the MOU for a period of one year with a focus on improving stability and sustainability. These improvements required ICANN to clarify its mission and responsibilities; to ensure transparency and accountability in its processes and decision making; to increase its responsiveness to Internet stakeholders; to develop an effective advisory role for governments; and to ensure adequate and stable financial and personnel resources to carry out its mission and responsibilities.

ICANN made strides during the past year towards developing into a more stable, transparent, and responsive organization. It completed a reform effort that resulted in structural adjustments and refinements to its decision-making processes designed to allow for greater transparency and responsiveness to all critical Internet stakeholders. In addition, the corporation hired a new Chief Executive Officer with both management expertise and experience in dealing with this unique organization. ICANN collaborated with governments to improve communication on public policy issues by establishing liaisons between its Governmental Advisory Committee and each of the ICANN supporting organizations.

While ICANN made progress, both the Department and ICANN recognize that there remains much to be accomplished in order for ICANN to evolve into the stable and sustainable management organization that it must be. The Department believes that the MOU, therefore, should be extended and amended to include milestones to ensure ICANN's steady progress towards that end.

These milestones would encompass the following areas of ICANN's development: (1) a strategic plan with goals for securing long-term sustainability of its critical domain name and numbering system management responsibilities; (2) a contingency plan to ensure continuity of essential domain name system operations in the event of the corporation's bankruptcy, dissolution, or any other catastrophic failure or natural disaster; (3) ICANN's relationship with the root server system operators to enhance the security of the root server system; (4) agreements with and more involvement from Regional Internet Registries, which are responsible for allocating numbering resources within their respective geographic regions; (5) accountability mechanisms such as arbitration procedures and selection of an ombudsman; (6) agreements with and more involvement from country code top level domain operators; and (7) an appropriate long-term strategy for selecting new top level domains.

If the MOU is amended in this manner, then ICANN should be afforded sufficient time to complete the agreed tasks. Thus, the Department intends to negotiate an extension of the MOU that is likely to exceed one year, while ensuring timely and steady progress is achieved. An extension of more than one year would allow for the completion and realization of structural and organizational changes that ICANN has initiated in the past year. It would also give ICANN sufficient time to seek and to provide opportunities for enhanced cooperation by all participants necessary to complete the tasks remaining under the MOU. The Department further is sympathetic to the view that a longer term for the MOU would permit ICANN to attract and to retain staff with the expertise critical to the success of this continued effort.

PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

The Department has long been concerned about the protection of intellectual property rights on the Internet. In order for the Internet to be a secure and stable network for electronic commerce, businesses must have confidence that their intellectual property can be protected in the online environment. The Department has worked for many years, domestically and internationally, to provide appropriate enforcement tools for U.S. intellectual property rights holders and to urge our trading partners to do the same.

In 1998, when the Department first set forth its statement of principles for private sector management of the Internet name and numbering system, it highlighted the importance of intellectual property issues. In particular, the Department's Statement of Policy on the Privatization of the Internet Domain Name System on the

Management of Internet Names and Addresses called for a dispute resolution policy to address cybersquatting as well as a “searchable database of registered domain names that provide information necessary to contact a domain name registrant when a conflict arises between a trademark holder and a domain name holder.”

The World Intellectual Property Organization (WIPO) responded to this call regarding cybersquatting by developing a Uniform Dispute Resolution Policy (UDRP) and recommending this policy to ICANN for consideration. The UDRP requires domain name registrants in all generic top level domains (such as .com, .org., .biz) to agree to an arbitration mechanism in the event that the domain name infringes a trademark holders rights. In 1999, ICANN adopted and implemented the UDRP as its first consensus policy. It is widely recognized as one of ICANN’s significant achievements.

The Department’s 1998 Statement of Policy also called for introduction of competition in the domain name registration market. In response, ICANN established a process in 1999 to accredit domain name retailers or registrars. This accreditation process for registrars was accepted by the Department and the U.S. intellectual property community as one avenue for addressing concerns regarding transparency and accountability in the domain name system. This process requires registrars to agree to collect and make available to the public contact information for domain name registrants.

WHOIS

This public domain name registrant database, known as the “WHOIS” database, serves many important public policy needs. For example, it allows intellectual property owners to determine the identity of those conducting piracy or trademark counterfeiting operations; Internet Service Providers, hosting companies, and network operators to maintain network security and investigate technical problems; law enforcement officials to investigate illegal activities online; and consumers to identify the commercial entity with whom they are dealing online. With regard to intellectual property owners, the WHOIS database provides a quick and effective way to reach a domain name registrant that might be engaged in intellectual property infringement.

Concern has been raised by privacy advocates and other national governments, however, about the administration of the WHOIS database, including the protection of the privacy of citizens who use the Internet; compliance with national laws that restrict the collection and availability of personal data; prevention of the use of WHOIS data for purposes of unsolicited commercial marketing; and prevention of personal contact information contained in the database from being used for purposes such as harassment or identity theft.

The Department of Commerce is working, along with the ICANN community, to explore the issues implicated by WHOIS and to find an appropriate balance among competing public policy interests to achieve a more accurate and available WHOIS database. A number of U.S. government agencies participate in a U.S. interagency working group that is examining what changes, if any, would improve the accuracy and availability of the WHOIS database. The Department’s National Telecommunications and Information Administration (NTIA) chairs that group, which also includes the U.S. Patent and Trademark Office (USPTO), the Federal Trade Commission, and the Department of Justice.

ICANN has provided a valuable international forum to seek consensus on WHOIS issues on a global scale. The Department participates in the ICANN discussions through its representation within the Governmental Advisory Committee. An NTIA representative sits on the Governmental Advisory Committee and works closely with the USPTO to ensure that the United States’ intellectual property interests are recognized and taken into account in ICANN’s policies.

Top Level Domain Registry Agreements

All ICANN agreements with generic top level domain registries include WHOIS database requirements. The newer registry agreements (e.g., .biz, .name, .pro) provide for more robust WHOIS data collection at the registry level. ICANN’s registrar accreditation agreements require registrars to collect, to maintain and to make publicly available, up-to-date WHOIS data for registrants in the generic top level domains. These agreements require registrars to have written agreements with each registrant to provide accurate registrant contact information, to update such data promptly, and to respond in a timely manner to a registrar’s request regarding the accuracy of such data. A registrant’s failure to meet these requirements constitutes a breach of this agreement that can result in the cancellation of that registrant’s domain name. In addition, ICANN adopted a new policy in June 2003, the WHOIS Data Reminder Policy (WDRP), which now requires all accredited registrars to con-

tact each registrant, at least annually, to confirm the accuracy of their contact information or to make necessary corrections. Failure to do so can result in domain name cancellation. This new policy goes into effect as of October 31, 2003 for existing accredited registrars. All new accredited registrars must comply with this policy as of the date of their agreement with ICANN.

In addition, ICANN has established a central mechanism for receiving complaints about false WHOIS data. The "WHOIS Data Problem Reports" system has been operational for almost 12 months. During that time, ICANN has received 15,458 problem reports, concerning 10,271 unique domain names (some names were the subject of multiple reports). ICANN forwards complaints received to the relevant registrar for investigation and resolution under the terms of the registrar accreditation agreement. While most of the reports concerned inaccurate WHOIS data, some of the reports were general queries or misdirected attempts by registrants to update their contact information with their registrar. At present, the total number of all registrations in generic top level domains is a little over 30 million names (registrations in .com represent a little less than 25 million of that number). Thus, if all of the more than 10,000 reports received by ICANN over the course of the past year represent inaccurate data, these complaints would total only 0.03% of all registrations. ICANN is currently working to improve the functionality of this system, including making it easier for registrars to process and report on the status of individual investigations and making the operations more transparent for persons submitting problem reports.

These contractual obligations and reporting mechanisms are important tools for ensuring continued access to accurate WHOIS data. Concern has recently been raised by users of this WHOIS data that some ICANN accredited registrars may not be abiding by the terms of their agreements with ICANN. We share these concerns, and are thus gratified that ICANN's new President and CEO, Dr. Paul Twomey, has demonstrated an understanding and commitment to resolving WHOIS issues, including enforcement of its registrar agreements. Enforcement should also improve as new staff is hired. Moreover, the new WHOIS complaint reporting system and newly adopted WDRP are important developments in improved WHOIS accuracy.

Lastly ICANN conducted an educational workshop at its June 2003 meeting to encourage dialogue within the ICANN community on WHOIS and to promote the development of consensus policies to address concerns. As a favorable response to this workshop, several stakeholder groups, including the intellectual property community, have begun additional work on the technical and policy aspects of collection and dissemination of WHOIS data.

Country Code Top Level Domains

Appropriate tools for intellectual property enforcement are equally vital in the context of country code top level domains. Sales of these country code top level domain names, such as those within .uk, are growing at a faster rate than sales of generic names, such as .com. Because it has very few agreements with operators of country code top level domains, ICANN can only attempt to influence best practices in these domains, including the development of accurate and available WHOIS databases. Moreover, registrar accreditation agreements currently apply only to registrations in generic top level domains. Through informational sessions and discussions on the many uses of the WHOIS database, such as the June 2003 workshop, the Department expects many country code top level domain operators to acquire a better appreciation for the expectations of other ICANN constituencies regarding the accuracy and availability of WHOIS data in those name spaces, and to adopt practices consistent with those expectations.

Achieving stable agreements with country code top level domain operators should be one of ICANN's top priorities. While ICANN continues to make progress towards establishing such agreements, forward movement has been slow. ICANN must develop a framework agreement that not only appeals to the majority of country code top level domain operators, but also recognizes differences in national law and other national sovereignty concerns. In this regard, the Department is pleased that the ICANN Board recently adopted bylaws creating a new supporting organization representing country code top level domain name operators. This supporting organization will be an important forum for ICANN to address policies on cross-cutting issues such as WHOIS and in working towards a country code framework agreement.

In the ICANN forum, the Department has actively encouraged the adoption of a dispute resolution policy to address cybersquatting as well as the collection and public availability of registrant contact information in country code top level domains. The Department uses its own agreement with the operator of the United States country code top level domain, ".us," as a model of the way that such a domain can

be administered consistent with intellectual property protection. Provisions in the .us contract with NeuStar, Inc., include a sunrise period for pre-registration of trademarks when the expanded name space came online, a dispute resolution procedure to address cybersquatting, and a robust WHOIS database of domain name registrant contact information. Moreover, the .us WHOIS database is centralized at the registry level to permit any interested party to search all registered names in .us without having to conduct multiple searches of the data collected by individual .us registrars.

Other International Efforts

The Department's efforts to protect intellectual property rights in the domain name system have not been limited to its relationship with ICANN. The Department, through the USPTO, participates in WIPO, an important global forum for the debate of intellectual property issues including those pertaining to the digital environment. At the request of the United States and other WIPO members, discussions on appropriate WHOIS policies for both generic and country code domain names have long been underway. In 2000, WIPO launched a program to assist country code top level domain managers in the design of appropriate domain name registration practices, including WHOIS database and dispute resolution procedures. In 2001, WIPO published Best Practice Guidelines for country code top level domain managers that set forth minimum standards for the protection of intellectual property in the country code top level domains. The WIPO guidelines will be an important resource for ICANN's new country code supporting organization.

The Department is also addressing these issues in bilateral free trade agreements by advocating that these agreements include commitments by governments that their country code top level domain operators will provide WHOIS-type registrant information and a cybersquatting dispute resolution procedure. As a result of this advocacy, such provisions were included in the free trade agreements between the United States and Singapore and the United States and Chile.

CONCLUSION

The Department remains committed to enforcement of intellectual property rights in the digital environment. We recognize that accurate and available WHOIS data is also a useful tool for law enforcement officials, network operators, and consumers, among others. For these reasons, the Department will continue to advocate in ICANN for a and other appropriate venues for a more accurate and available WHOIS database and will work to ensure that U.S. intellectual property rights holders are provided appropriate enforcement tools in generic and country code top level domains.

Mr. SMITH. Let me address my first question to Mr. Metalitz and Mr. Edelman. Mr. Metalitz, you mentioned that you thought the Whois database was and is deplorably bad. Mr. Edelman, you called the Whois database substantially fiction. Do you think that any of the seven milestones mentioned by the Department of Commerce—we just heard about five and there are two others you may be familiar with—are any of those milestones or anything that you've heard or seen from the Department of Commerce to date convinced you that we're on the verge of having accurate, reliable database—Whois database that is going to be helpful in the future? Mr. Metalitz?

Mr. METALITZ. Mr. Chairman, the—none of the seven milestones that are listed in the Commerce Department's written testimony address this directly or even indirectly.

Two of them do talk about entering into new agreements, in one case with the country code top-level domains and in another case with the regional Internet registries, and this is why we think the question of contract enforcement is so important in evaluating ICANN at this point. But certainly in the list of seven milestones that were in the written testimony, there is nothing that directly relates to Whois or that will have much impact in this area.

Mr. SMITH. Mr. Edelman?

Mr. EDELMAN. I stand by Mr. Metalitz's comments.

Mr. SMITH. Okay. Fair enough. Let me address my next question both to Mr. Edelman and Mr. Farnan, and this goes to the Department of Commerce assertion that ICANN provided inaccurate data—complaint record amounts to only about three one-hundredths of 1 percent. That is contradictory to the testimony that you have given, Mr. Edelman—as far as that goes, testimony of Mr. Metalitz. But Mr. Farnan said in his testimony that the Whois database was—the ICANN provided Whois database was often inaccurate and incomplete in cases that you needed it to be complete and accurate.

Mr. Edelman and Mr. Farnan, what do you think of that suggestion that the inaccurate data is just a small percentage of the overall? Mr. Edelman?

Mr. EDELMAN. First, I don't want to mischaracterize Mr. Kassinger's testimony. As I read it here on page four, he points out that if one takes the quotient of the number of complaints received to the number of domains in existence—that is about 10,000 divided by about 30 million—the result is three one-hundredths of a percent.

Mr. SMITH. Right.

Mr. EDELMAN. To be sure, no one is saying that every domain with invalid Whois data has been the subject of a complaint. Quite the contrary.

Mr. SMITH. That's the point.

Mr. EDELMAN. So that would not be a statistic that would really provide any information whatsoever as to the number of domains with invalid Whois data. It's a difficult subject to estimate. I've attempted to do it on some occasions. Certainly, I had no trouble in a project conducted while a full-time college student in identifying 12,000 domains in the space of perhaps just a few hours of work designing the algorithm to do the research and then some additional work preparing the lists and publishing them.

I suspect the true answer is on the order of several percent. I wouldn't be surprised if it was as high as 10 percent. These are on the order of two to even three orders of magnitude larger than the written testimony would suggest.

Mr. SMITH. Okay. Thank you, Mr. Edelman.

Mr. Farnan?

Mr. FARNAN. Sir, based on what we do for a living at the FBI, we don't accumulate the kind of statistics that would be directly responsive to what Mr. Kassinger testified to. But what I can tell you is this. When we go to Whois, we access Whois, we would not take the information directly from Whois and put it instantly into an affidavit, for example, or other kind of court document. We would verify that what we're getting from Whois is accurate, and we do that on a regular basis. So we would not rely on Whois explicitly. That's probably the best I can do to answer that one.

Mr. SMITH. Okay. Thank you, Mr. Farnan.

Mr. Kassinger, let's pursue that question of how accurate the Whois database is. Would you agree that your three one-hundredths of 1 percent is not representative of an accurate database?

Mr. KASSINGER. The data were not put in that testimony to suggest that it was, and I think the previous witness identified that

correctly. That may just be the tip of the iceberg. However, I'm very interested—

Mr. SMITH. If it's just the tip of the iceberg, why did you use it, or why did you not admit to a larger inaccuracy?

Mr. KASSINGER. The point wasn't to assert the value of inaccuracy one way or the other. The point was to show that the system is up and running, and I understand that it is ramping up and they're getting more and more names. It is not the answer to inaccurate data.

But Mr. Chairman, if I might say, we heard a characterization of the problem as—of the Whois database as substantially fiction, and yet the high-end number we've just gotten here was 10 percent. Now, one of the real issues here is we don't know how widespread it is. Clearly, it's a large problem. I think one of the suggestions made in testimony earlier was to invest in resources and identifying the number of registrars that are bad actors and developing better data. We would support that.

Mr. SMITH. Yes. I think you made a fair point about the 10 percent figure used by Mr. Edelman, and maybe he can refer to it a little bit later on, and I thought of substantial fiction and thought it might be more than 10 percent. On the other hand, I think it's also a fair point to make that your mentioning that three one-hundredths of 1 percent was a little misleading when, in fact, those were just sort of self-initiated complaints and really not a real reflection on the inaccuracy found at the Whois database.

My time is up, but I'll return with some more questions in a minute. The gentleman from California, Mr. Berman, is recognized for his questions.

Mr. BERMAN. Thank you, Mr. Chairman.

At least in this round, I'd like to start with Mr. Edelman. Just first of all, thank you very much for coming in, for your—the candid nature of your testimony. I think it dispels a lot of the rationalizations for failing to improve Whois and gets to the real reason why we have seen so little progress on this issue. I'd like to ask you a few questions just—in some cases they repeat points you make, but I think sometimes it's worth hearing them several times.

Just on your first point, Mr. Smith, the Chairman, brought this out. For those of us who are really stupid in math, two or three times the order of magnitude is different than two or three times. I take it you're distinguishing between three-hundredths of 1 percent of complaints received and what you think might very well be two or 3 percent, and perhaps up to 10 percent, of the 30 million domain names have misleading information.

Mr. EDELMAN. That's quite—

Mr. BERMAN. It's not a multiple, it's an exponential kind of—

Mr. EDELMAN. It's an exponential, and order of magnitude refers to a power of ten, so two orders of magnitude would be a factor of 100 and three a factor of 1,000.

Mr. BERMAN. That's what I wanted. Thank you. Okay. I knew there was something there— [Laughter.]

—but I couldn't say it. Do you believe that accurate and complete Whois databases can exist with adequate privacy protections, and if so, could you elaborate?

Mr. EDELMAN. Absolutely. There are a number of ways that accurate Whois data could take place at the same time as individual privacy is protected. The easiest way to think about this is a post office box operated by the U.S. Postal Service. It's quite easy to register a box at the post office and then have the post office receive your mail, perhaps even without distributing your name to those organizations or companies sending you mail.

Similarly, one can register a domain name with a registrar that provides a sort of escrow service whereby the registrar puts its own name in place of the registrant's name and accepts the legal responsibility for passing communications on to the actual registrar as received. This takes place—

Mr. BERMAN. Actual registrar or actual registrant?

Mr. EDELMAN. Actual registrant. Please excuse my mistake. And this takes place already for a very small supplemental fee. Registrar "GoDaddy," one of the largest five registrars currently operating, has this service. Others use their lawyers. You can imagine any of a number of other services that could provide this escrow facility.

Mr. BERMAN. Thank you. Do reasonably effective and inexpensive mechanisms exist with which registrars could substantially improve the accuracy and completeness of Whois data?

Mr. EDELMAN. Yes. The irony is that many registrars are already using such systems to make sure that they get paid. When they receive a credit card number, they want to verify that that credit card is actually a valid credit card, one for which they will receive payment from Visa or Master Card, so they cross-check the name on the credit card with the address initially offered. At that point, there is good reason to believe that someone, at least, has this credit card with that name. Perhaps it's stolen, but that may be a de minimis problem.

On the other hand, they subsequently allow changes. You could change your registrant name, certainly your address and your phone number, at which point your Whois data could be full of intentional errors.

Mr. BERMAN. In your opinion, is cost and potential lost revenue one of the major reasons registrars fail to verify the accuracy and completeness of Whois data? In other words, is it at the present time, given the nature of enforcement, is it in their registrars' financial interest not to verify the accuracy and completeness of Whois data beyond their billing and collection purposes for registration?

Mr. EDELMAN. I think the cost of conducting verification is one of the factors at issue here, but I'm not sure it's the largest factor. I think the largest factor is probably that any registrar conducting these sorts of verifications would tend to drive customers away. The very lucrative customers registering 10,000 domains, perhaps putting pornography on all of them and attempting to encourage children to access them, these are good customers to a registrar because they pay their fees every year and they have a large number of domains. One wouldn't want to send away that sort of customer unless it was absolutely necessary, say, due to active enforcement efforts by ICANN. And so we see registrars continuing to serve that sort of customer because, at least so far, they can.

Mr. BERMAN. So that I take from those comments that this might be the classic case where effective minimum standards and enforcement of those standards removes the competitive advantage of—of no—of inadequate efforts to get accurate information.

Mr. EDELMAN. Precisely. Without that sort of regulation, there would tend to be a race to the bottom, which I believe is what we've seen so far.

Mr. SMITH. Thank you, Mr. Berman.

The gentleman from Texas, Mr. Carter, is recognized for his questions. The gentlewoman from Wisconsin, Ms. Baldwin, is recognized.

Ms. BALDWIN. Thank you, Mr. Chairman.

Mr. KASSINGER, I wanted to use the opportunity presented by this hearing to call your personal attention to a related matter, a matter that Senator Cantwell raised in a recent Senate Subcommittee hearing and which has been addressed in legislation introduced in this House by Representatives Baird, Pickering, Inslee, McDermott, and Case, embodied in H.R. 2521.

ICANN has indicated that it will soon grant an exclusive contract to one company to process requests by consumers for back-order domain names. In an August 15 letter, a written response to Senator Cantwell's question, Assistant Commerce Secretary Nancy Victory assured that Senate Subcommittee that the Department was authorized to evaluate in advance of granting approval how such activities undertaken by ICANN could affect the public interest.

I'm concerned about whether this exclusive contract is necessary since the current system has resulted in competition among a multitude of small business registrars, domain registrars, and competition has also led to lower prices for domain names on this secondary or back-order market.

Therefore, I am asking that you evaluate the impact of the ICANN proposal, the impact that it will have on consumers and the nearly 100 small and medium-sized businesses that are currently competing in this business market and report back to us on the matter before the exclusive contract is approved. Obviously, I'm not asking for you to provide that analysis immediately. I understand that you cannot do so today. But I would note that significant time sensitivity does exist and I would welcome your cooperation in that matter.

Mr. KASSINGER. Congresswoman Baldwin, we certainly will get back to you on that. If I understand the subject of your question correctly, it has to do with the proposed Verisign WLS contract—

Ms. BALDWIN. Yes.

Mr. KASSINGER. That, first of all, I should clarify, is not an ICANN proposal. It's a Verisign proposal that they must submit and work through the ICANN process for approval. I'm not sure it's exclusive. I just think it's a proposed service that they would have to get approved.

By virtue of our legacy agreements, we do, in that particular situation, have a right and responsibility to review the ultimate agreement and we will do so. We have not been presented with such an agreement yet so there's nothing yet to analyze. But when

it is presented, if and when it's presented, we certainly will analyze it and get back to you about that.

Ms. BALDWIN. I think part of my concern is the appearance that it's gearing up and ready to be unfolded on a very short timeline, maybe on a 1-year trial basis. But we're certainly eager to see the results of a thorough analysis, especially its impact on consumers in terms of price as well as on the multitude of small and medium-sized businesses that are potentially going to be displaced by this activity.

Mr. SMITH. Thank you, Ms. Baldwin.

Mr. Kassinger, let me return to a couple of the points that I was making before, but let me quote from your written testimony, where you say registrants that fail to provide such information, meaning accurate database information, to their registrar run the risk of losing their domain name. Failure to do so can result in domain name cancellation.

Why is it that ICANN seems not to enforce the contract with the registrars? Why has there not been a single cancellation? Why has not a single accreditation been revoked? It seems to me that that would indicate pretty strongly that there's not a real seriousness of intent by ICANN or by the Department of Commerce to have an accurate and reliable Whois database.

Mr. KASSINGER. Mr. Chairman, I don't know fully the answer to your question of why ICANN has approached the problems evidently raised by the Administration of the registrar agreements, in the way they have, but I think there are pretty clearly a couple of forces at work.

One is resources. There are roughly 170 registrar agreements. A substantial number of those are overseas. The threat of cancellation of an RAA on the basis of breach is a pretty serious one and ICANN understandably has to approach that carefully. It could find itself pretty quickly in a lot of litigation, which it's not, in my judgment, equipped to handle, financially or otherwise.

So I think the approach of ICANN has been to work through the various constituencies to identify reasons why, as mentioned earlier, there seems to be a number of disincentives to adhere to these agreements. I think Congressman Berman used the phrase preventive—prevention earlier, and I completely agree. In general, it's much better to use preventive medicine than it is to try to cure a problem later, and I think that generally has been the approach ICANN has been trying to follow.

Mr. SMITH. Mr. Kassinger, if you've been using prevention, it hasn't worked, and if you don't enforce, the message you send is that you don't care or it's not important. And regardless of the inaccuracy rate, whether it's 10 percent plus or minus, that's still way too high. My guess is it could be more from anecdotal information. And 10 percent, as I say, is a huge number when you look at how much, or how much that data is relied upon by so many individuals and so many organizations.

But let me address my question maybe to Mr. Metalitz, Mr. Edelman, and perhaps Mr. Farnan, as well. What is your opinion? If there is no enforcement, if there is no revocation of accreditation, if there is no sort of effort to have registrars comply with the contracts that they have with ICANN, do you think that that's part

of what accounts for the substantial inaccuracies in the Whois database? Mr. Metalitz?

Mr. METALITZ. I think it's definitely a causative factor. I think this really gets back to the questioning that Mr. Berman posed to Mr. Edelman. One of the reasons why registrars accept so much bad data is that there's no penalty for doing so. Not only do they not have to expend even the minimal cost of verifying data, but they—there's no penalty if they just let anybody come in and put any data they want in the Whois database. So if that provision were enforced, if action were taken or case files were opened to enforce those provisions against some registrars, I think it would have a salutary effect.

Mr. SMITH. Okay. Mr. Edelman?

Mr. EDELMAN. I agree, of course, with Mr. Metalitz. The core problem here is a lack of oversight by ICANN, encouraging the registrars to accept anyone who comes with money or credit card in hand wanting to register a domain, be it with truthful or with intentionally invalid Whois data. A registrar has the choice between making some money or turning away a would-be customer to one of its competitors. In that context, it's not hard to understand why the registrars always choose the former.

Mr. SMITH. Okay. Thank you, Mr. Edelman.

Mr. Farnan?

Mr. FARNAN. Sir, from a law enforcement perspective, anything that can be done that would increase the accuracy of the information in Whois would be helpful. Anything contrary to that is not helpful, and I walk a very fine line between suggesting how that can be fixed, which I don't believe is our place from the law enforcement community, but our point is that to the extent that the information is inaccurate causes us to expend more resources and more time to find the accurate data.

Mr. SMITH. Okay. Thank you, Mr. Farnan.

Mr. KASSINGER, let me conclude with a question to you, but in passing, let me follow up on the word "resources" that you used and Mr. Farnan just used. It seems to me that no matter how thin the resources, there just isn't really any good explanation for not a single instance of going after a bad actor here, not a single instance of revocation or loss of accreditation or whatever, and regardless of—you can offer excuses, but I'm not sure it's a real explanation.

As far as the inaccurate data goes, and I've forgotten which witness suggested it in their testimony, but would you be willing to have an outside audit conduct a study of just—as to the extent of the inaccurate database of—Whois database?

Mr. KASSINGER. I think the development of better data on the extent of this problem is essential, and if that's one way of getting at it, that would be welcome. I don't know who pays for that. We'd have to figure that out.

Mr. SMITH. But in theory, you're not opposed to it?

Mr. KASSINGER. In theory, I'm not opposed to it.

Mr. SMITH. Okay. Thank you, Mr. KASSINGER. I know Mr. Berman has a couple questions, as well.

Mr. BERMAN. Thank you, Mr. Chairman.

You talked about resources. Mr. Edelman mentioned a specific act that registrars frequently do, which is to verify the name and address of the credit card holder submitting the credit card payment. Would it cost a lot and take a lot of effort for a registrar to at least determine the information they have received in trying to verify the validity of the credit card, they cross-check it with the Whois database to make sure that's the same name and address used on the Whois database?

Mr. KASSINGER. Technically, that sounds quite feasible to me. I'm honestly not an expert in the financing of setting up those cross-checking systems. I know the registrars argue that there are thin margins in this business and they have invested a lot of money. I don't know the accuracy of their claims.

Mr. BERMAN. This seems like a pretty thin effort they would have to undertake to simply do that, but that's more a comment.

What's the status of the draft MOU? Are we sort of whistling in the wind here, nothing we say, no new insights? Obviously, you've gotten some insights from your written testimony to your testimony today, because the written testimony sort of gave a, there are no problems, things are okay, air to it, and your testimony today is very, I think, useful and helpful in acknowledging the problem could be far greater than perhaps we concluded from reading your testimony and that there are many problems still remaining. Is there a chance through this draft MOU for Commerce, if it wanted to, to propose some additional provisions not now in the draft MOU?

Mr. KASSINGER. Uh—

Mr. BERMAN. In other words, is this the final MOU? [Laughter.]

Mr. KASSINGER. There is no MOU.

Mr. BERMAN. There isn't?

Mr. KASSINGER. Certainly, this Subcommittee is never whistling in the wind, Mr. Berman. We listen carefully and we value your input. Here's the situation.

We have spent a lot of time over the last 3 months internally and working with ICANN management to identify the issues that would go into an MOU. We have been drafting an MOU. We have not presented a draft MOU to ICANN yet. We anticipate doing that in the near future. So yes, this is an issue on the table and—

Mr. BERMAN. Well, let me make a suggestion, not that this should be the only one. I think a lot of things have been said here that Commerce might want to consider. But I'm told that several services, such as Fraudit, operated by Alice's Registry, exist to improve the accuracy and completeness of Whois data. Mr. Edelman notes that no registrar has thus far opted to use those services.

Why shouldn't the Commerce ICANN MOU require registrars to use such services or take other proactive measures, like cross-checking the credit card information with the Whois database information or any of a number of things, or not make it a choice between doing nothing and having ICANN have to cancel, but imposing a series of fines and other kinds of sanctions on registrars for failing to do things that don't—you know, that are short of the registrar death penalty but still can provide some meaningful deterrence for—that would incentivize registrars to do what they should be doing? Why couldn't the MOU have these kinds of provisions?

Mr. KASSINGER. It misconceives the nature of the MOU is fundamentally the reason, Mr. Berman. We actually are attracted to a number of the ideas that Mr. Edelman mentioned and others have in our interagency committee. Those are the kinds of things we're looking at proposing within ICANN to impose. The MOU does not—we are not a regulator. The MOU is not a regulatory instrument. It is a contract where we define certain goals and expectations. Now, that's how we might get at some of this, defining what we expect, but not going to the level of detail of you shall impose a fine for, you know, in X circumstances.

Mr. BERMAN. What do you mean? I mean, Department of Defense is a contractor, not a regulator, but it certainly imposes on its contractors certain kinds of penalties for not meeting its contract terms. Why couldn't this be—why can't you sort of expand the horizons of this MOU to include some of these things, including obligating uses of those services?

Mr. KASSINGER. Well, you know, we're not in contractual relationship or privity with the registrars, so we're not—

Mr. BERMAN. No, I'm talking about with ICANN.

Mr. KASSINGER. I raise, you know, query, what's the point of penalizing financially ICANN? This is an organization—

Mr. BERMAN. No. You're requiring ICANN, and ICANN is agreeing through this Memorandum of Understanding, to undertake provisions in its contracts with its registrars to impose penalties short of cancellation for failure to do certain relatively simple, relatively low-cost kinds of things to improve the accuracy of the Whois database.

Mr. KASSINGER. Using the MOU as an instrument to secure better compliance with Whois data is in the realm of possibility and should be considered. I do not think the MOU is an appropriate instrument to specify to ICANN precisely how it carries out the roles that we envision for it.

ICANN is—you know, we're trying to privatize this. We're trying to get them to stand up on their own and figure out for themselves how to walk and run. They have a lot of constituencies with whom they deal. It's—in the next 30 days to figure out what the appropriate penalty structure should be and then impose that through the MOU, I don't think would be a wise course of action.

Mr. BERMAN. Well, I'm disappointed by your answer. Mr. Metalitz?

Mr. METALITZ. Mr. Berman, if I could just add something on that, I can understand the reluctance of the Commerce Department to get into a lot of detail in the MOU, but as Mr. Kassinger said, the model should be that ICANN would work this out itself and come to some solution like this. But in that regard, it's very discouraging to have to report that many of the solutions that are being talked about this afternoon have been proposed within ICANN and they've never gotten anywhere.

We've proposed intermediate sanctions, the idea that for violation of the registrar accreditation agreement, there should be some penalty short of disaccreditation. We've proposed that, and I don't think an idea that's been placed on the table in ICANN has ever been shot down so fast as that one. Registrars and registries didn't

want to hear of it, and since there was no consensus, we couldn't proceed any farther.

Some of the suggestions that Mr. Edelman made in his testimony, which I think are very good ones, we put forward. The intellectual property constituency put forward the idea that if you catch John Zuccarini in one false Whois registration, why not cancel all 8,000 of them that are registered exactly the same way? That got shot down, as well.

So I think there has been a lot of opportunity for ICANN to put its house in order and put some of these rules into effect and it may be that the MOU does need to be somewhat more detailed in some of these areas in order to perhaps nudge ICANN in the right direction.

Mr. BERMAN. In closing, since my red light has probably gone off—

Mr. SMITH. Long ago.

Mr. BERMAN.—an entity which at this point is doing very little to meet its lip service to commitment to improving the Whois database, the Department of Commerce is trying to privatize without any serious demonstration by that entity that it will do something to give meaning to what it pays lip service to. That's just an off the top of my head conclusion, not a question. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Berman.

Mr. Kassinger, you just—I'm going to interject. You mentioned that you wanted ICANN to walk before they run, or walk and then run. When it comes to enforcement, they're still crawling, and I think your MOU is going to have to include an enforcement component or we will not be convinced that you are really heeding a lot of serious concerns, not only by us, but by every other organization that has any connection to the Whois database. I think you're going to need to reassure us with some more attention given to enforcement.

The gentleman from Texas, Mr. Carter.

Mr. CARTER. I think this is the only way I can talk to you, if this thing over here doesn't set off that noise again. I happen to believe in enforcement, and what I can't understand as I hear this is that at least someone could be starting to pressure for enforcement. They're not crawling. They're not even out of the gate.

It seems to me that the thing—a suggestion, and maybe it's a bad suggestion, you tell me, Mr. Edelman's done some research where he's identified several thousand of these false sites. So you've got somebody who's already done some research for you. Why not send notice and put them on notice that it's the Department of Commerce's position that they should enforce against those identified sites, and you provide them to them, with the idea to—and by noticing them to correct their data, give them 30 days, and if not, to strike their domain.

And then put that—publish that. That certainly is going to get the information out to the entire world, and those people who innocently gave bad data are going to say, wow, I'm going to get in here and correct my data because I'm innocent on this. I just didn't—really didn't really intend it that way, and there may be millions of those, I don't know. But those who are intentionally trying to de-

ceive will then be put on notice if deception will come with a death penalty, and I happen to believe in the death penalty.

Mr. KASSINGER. Mr. Carter, just to clarify again, the Commerce Department doesn't have a direct relationship with the registrars. I think we do from time to time get complaints about specific misleading or false registrations and we do pass those to ICANN or the registrar or registry operator that's relevant. But it is up to those organizations to take action, and I think the broader question here is what should we, as an agency, be doing to move those groups along in the direction of stiffer enforcement.

Mr. CARTER. Well, if the Commerce of the United States requires that we have accurate data, if the chief law enforcement or law enforcer—yes, I guess you're law enforcers—are concerned about the lack of data as they try to operate within the realm that they operate, then what is the role of Commerce in telling this private entity, you're not doing your job. This is what you're here for. You're not doing your job. We're concerned about it. Do you want the Government to get in the middle of your business or are you going to clean up your act? And that's kind of where we are right now, it looks like to me. And to me, someone's got to speak up somewhere and say, this is not working, and you seem to have, at least by your relationship with them, some influence over them and should be able to make suggestions to that effect.

Mr. KASSINGER. And we do make those suggestions. We are actively involved in a number of ICANN groups that are working on this very issue and we do press those views vigorously. But we are—again, we're not the regulator of ICANN, so—but it—

Mr. CARTER. Well, somebody else certainly could get to be the regulator of ICANN in a heartbeat if it doesn't get doing its job.

Mr. KASSINGER. Well, I think ICANN dissolves in that case and we try a different experiment, so hopefully, that—we can solve this issue without getting to that point.

Mr. CARTER. And that's a worldwide death penalty.

Mr. KASSINGER. That's right.

Mr. CARTER. It's okay with me.

Mr. SMITH. Thank you, Mr. Carter, for those good points.

We thank you all. It was excellent testimony. And let me reassure the witnesses and also the audience that we are not going to drop this subject. Mr. Kassinger, we will be watching closely, of course, what the Department of Commerce does, also what ICANN does or does not do, and if we have to take appropriate action, we'll do so.

As Mr. Carter suggested, you know, ignoring the inaccuracies in the Whois database is not an option and I hope that—and one way I know for you all to show that you're not ignoring the problem is, in fact, to have better enforcement. I think a little enforcement will go a long ways, by the way, as far as getting more accurate information and having it more reliable and more accessible.

Before adjourning, I would like to include in the record a statement submitted by Margie Milam, General Counsel for eMarkmonitor, Inc.

[The letter from Ms. Milam follows:]

September 3, 2003

Via E-mail and U.S. Mail

The Honorable Lamar S. Smith
Chairman, Subcommittee on Courts,
The Internet, and Intellectual Property
Committee of the Judiciary
United States House of Representatives
B-351A, Rayburn House Office Building
Washington, D.C.

Attn: David Whitney

Re: WHOIS

Dear Congressman Smith:

EMarkmonitor, Inc. ("Markmonitor") respectfully submits the following statement to be included in the public record pertaining to the WHOIS hearings scheduled to take place tomorrow before the Subcommittee on Courts, the Internet and Intellectual Property, Committee of the Judiciary.

Markmonitor is an ICANN accredited registrar based in Boise Idaho serving the corporate domain registration market. Markmonitor is also a leading provider of research products and services that are used by the legal and law enforcement community to identify fraudulent, criminal, and intellectual property infringement activity over the Internet. As a result, Markmonitor has a unique perspective, different than other ICANN-accredited registrars, with respect to WHOIS issues.

Markmonitor's products and services are based in part on WHOIS information purchased on a bulk basis through the bulk access provisions contained in the ICANN Registrar Accreditation Agreement ("RAA"). Markmonitor is one of several service providers that rely on the bulk-access provisions to develop reports that help identify cyber-criminals, cybersquatters and other persons that may use the Internet for unlawful or illegal purposes. Other service providers include some of the nations largest legal publishing companies. Markmonitor's clients include Fortune 100 companies and financial institutions that use its reports and services to protect their customers from instances of fraud and to enforce civil laws relating to counterfeit goods, copyright and trademark abuse.

For example, reports generated from bulk WHOIS data have been used to investigate recent identity theft scams plaguing the banking industry known as "phishing." Under this scheme, cyber-criminals attempt to steal the identity and confidential information of online banking consumers. Phishing involves registering a domain name similar to that of a famous bank and copying the look and feel of the bank site. Consumers are then lured through an e-mail to

visit the fraudulent site and are prompted to provide their confidential information, which is used to siphon money from the consumer's actual bank account. Reports utilizing bulk WHOIS information can be instrumental in uncovering the identity of the cyber-criminal as well as other financial institution web sites being targeted.

Recently, several of the largest ICANN accredited registrars have changed their policies regarding access to their WHOIS Records on a bulk basis. Some have revised their agreements to include onerous provisions intended to discourage the purchase of the data altogether. For example, some bulk access agreements include liquidated damages in the amount of \$1,000,000 per breach. Other agreements unreasonably limit the use of the data contrary to the applicable ICANN agreements. Some registrars refuse to provide the data altogether. These actions have had an anti-competitive impact in that several major service providers have ceased providing their value-added services altogether. This has adversely affected the legal and law enforcement community which have relied on these services for investigative purposes. As a result of these recent events, ICANN should take action to enforce the bulk access provisions of the RAA.

Retaining bulk access to WHOIS for value-added service providers ensures that up-to-date and complete information is available to the legal community and law enforcement community. Service providers like Markmonitor have developed sophisticated search technology adept at searching databases to present information to the end-user that would otherwise not be obtainable through the standard public WHOIS access available through registrars. For example, a domain ownership WHOIS search could identify other domain names owned by a particular registrant, which can support a UDRP claimant in proving that such registrant is a cybersquatter. This advanced search capability is difficult to achieve if service providers do not have access to WHOIS data on a bulk basis. Without access to WHOIS data, the ability to enforce the Anti-Cybersquatting Consumer Protection Act, the Truth in Domain Names Act and other federal laws will be greatly reduced.

It is essential that public access to WHOIS data, through bulk access and through Port 43 web access, continue to be maintained. WHOIS information has been publicly available since the initial commercial adoption of the Internet and many individuals, businesses, non-profit organizations and governmental agencies have relied on such access to confirm the identity of website operators with whom they do business. In addition, Markmonitor believes that the current WHOIS system should be supplemented with adequate enforcement of the applicable provisions of the RAA.

Thank you for the opportunity to present Markmonitor's point of view on this important issue. If you require further information regarding the foregoing, please contact the undersigned at the phone number provided above.

Sincerely,

Margie Milam
General Counsel
eMarkmonitor, Inc.

Mr. SMITH. I would also like to include a statement from the International Trademark Association.

[The prepared statement of the International Trademark Association follows:]

PREPARED STATEMENT OF THE INTERNATIONAL TRADEMARK ASSOCIATION

Mr. Chairman, Congressman Berman, and Members of the Subcommittee on Courts, the Internet, and Intellectual Property:

The International Trademark Association (INTA) is pleased to submit this statement in connection with the subcommittee's oversight of intellectual property safeguards on the Internet. We thank the subcommittee for addressing this issue and for its letter of August 8, 2003, to Secretary of Commerce Donald Evans regarding developments that affect the operation of the Internet.

INTA's statement will comment on: (1) the role of the Internet Corporation for Assigned Names and Numbers (ICANN) in the administration of the domain name system (DNS); (2) Whois data and ICANN policies relating to access to the data, enforcement of those policies, and what can be done to improve enforcement; and (3) the need for uniformity in country code top-level domain name policies. We respectfully request that our statement be made part of the record of today's hearing.

About INTA

INTA is a 125-year-old not-for-profit organization comprised of over 4,400 member companies and firms. It is the largest organization in the world dedicated solely to the interests of trademark owners. The membership of INTA, which crosses all industry lines and includes both manufacturers and retailers, values the essential role that trademarks play in promoting effective commerce, protecting the interests of consumers, and encouraging free and fair competition. During the ongoing international debate on the running of the DNS, INTA has served as the voice of trademark owners in the United States and around the globe, working to ensure that their trademarks are protected and, more importantly, that consumers have a safe and reliable choice in cyberspace.

The DNS and ICANN's Role in Its Administration

The DNS is what allows Internet users to "surf" through cyberspace using familiar strings of letters and numbers as their guide. Very often, these identifiers take the form of trademarks (e.g., <http://www.inta.org>). In June 1998, through a policy statement known as the "White Paper," the U.S. government stated its intent to transfer management of the DNS to the private sector.¹ In November 1998, on behalf of the government, the Department of Commerce (DOC) entered into a memorandum of understanding (MOU) with ICANN, recognizing ICANN as the private, not-for-profit entity to which the government would transfer responsibility for DNS management. The MOU is renewed on an annual basis and is now set to expire on September 20, 2003.²

ICANN's role is necessarily one of both policy and technology. The technical and policy coordinating function performed by ICANN has helped to foster consumer confidence in the Internet as a means for conducting business in a simple, quick, reliable, and easy-to-understand manner. ICANN, through its administration of the DNS, provides a single avenue, whether

¹ <http://www.icann.org/general/white-paper-05jun98.htm>.

² Amendment 5 to the MOU can be found at <http://www.icann.org/general/amend5-ipamou-19sep02.htm>.

through meetings, working groups, or even its own website, for stakeholders of all backgrounds and interests to come together and voice concerns, create dialogues, and hopefully build common ground on matters critical to the future of the stability of the DNS for all users. It is commonality and standards, after all, which allow the Internet to serve as a global communications medium.

In promoting the stability of the Internet, ICANN has simultaneously taken steps to ensure proper conditions for protecting trademarks and, in turn, enhancing consumer protection. INTA applauds this decision. Tools such as the Uniform Dispute Resolution Policy (UDRP), which was put in place by ICANN in late 1999, have proven to be valuable means for trademark owners to address piracy and online consumer fraud. ICANN moved forward with these safeguards after consultation with user groups and with the intent of ensuring a stable Internet.

Whois Data

A Definition of Whois and Trademark Owner Use of the Data

The protection of brands and consumers in cyberspace and the stability of the Internet do not end with the UDRP, however. There remain several challenges that lie ahead, the solution to which will promote greater online stability; in particular, ensuring access to accurate contact data on registered domain names. This data is typically referred to as “Whois.” Whois has any number of important uses, including law enforcement, consumer protection, and the protection of intellectual property rights. Trademark owners value Whois data in order to resolve domain name disputes (e.g., cybersquatting),³ learn the contact details for owners of websites offering counterfeit products or other infringement of intellectual property, manage trademark portfolios, provide due diligence on corporate acquisitions, and identify company assets in insolvencies/bankruptcies.

Contractual Provisions and Policies Relating to Whois

The need for “trademark owners and domain name registrants and others”⁴ to have access to Whois was first addressed in the U.S. Government’s White Paper, which laid out the ground rules for private sector management of the DNS. The White Paper stated:

We [the U.S. Government] anticipate that the policies established by the new corporation [ICANN] would provide that [the] following information would be included in all registry databases and available to anyone with access to the Internet.⁵

³The data from Whois is crucial to learning the identity of a cybersquatter and establishing a case under both the UDRP and the *Anticybersquatting Consumer Protection Act*, a measure that originated with this subcommittee and was signed into law in November 1999. Pub. L. No. 106-113, § 3002, 113 Stat. 1501, 1537 (1999) (amending 15 U.S.C. § 1125).

⁴*Supra* note 1.

⁵*Id.*

ICANN, upon its formation and as part of its initiative to expand the number of domain name registrars,⁶ crafted the Registrar Accreditation Agreement (RAA),⁷ a contract between itself and domain name registrars that addresses the obligations ICANN accredited registrars have with respect to domain names registered in the global top-level domain (gTLD) space. This includes the familiar suffixes of .com, .net, and .org, as well as the recently introduced .info, .biz, .name, .pro, .museum, .coop, and .aero. Among the RAA obligations are compliance with the UDRP⁸ and the provision of Whois data.⁹ Both are in accordance with the precepts of the White Paper.

Today there are basically two types of Whois: (1) free, interactive, publicly accessible web-based Whois data that can be found by going to any registrar's website, finding the icon labeled "Whois," "clicking," and typing in a particular domain name;¹⁰ and (2) bulk Whois data that is the whole of a particular registrar's database, which can be purchased from a registrar by a third party for an annual fee not to exceed \$10,000.¹¹ Trademark owners use both types of Whois. Trademark search firms in particular purchase bulk Whois data in order to provide services to trademark owners, such as investigation of alleged cybersquatters, particularly to show whether the cybersquatter has a pattern of registering multiple domain names incorporating the trademarks of others. ICANN accredited registrars are required to have all of their registrants enter into an agreement wherein each registrant "shall provide to Registrar accurate and reliable contact details and promptly correct and update" those details during the term of the registration.¹²

Problems with Whois: Accuracy and Accessibility

Unfortunately, despite the RAA requirement that registrants provide "accurate and reliable contact details," trademark owners have for many years been encountering instances of inaccurate or missing data often from fictitious entities listing false addresses, as well as information that is simply out of date. These are just a few examples of bad data that trademark owners have recently come across:

- (1) In a recent UDRP case involving the cybersquatting of www.nhl.penguins.com, the individuals listed as administrative and technical contacts for the contested domain name, Allen Ginsberg and Charles Bukowski, respectively, are the names of deceased poets from the American "Beat Generation."¹³ The contact address listed in the Whois records was

⁶ Today there are approximately 167 ICANN accredited registrars from 25 countries.

⁷ <http://www.icann.org/registrars/accredited-list.html>.

⁸ RAA, at <http://www.icann.org/registrars/ra-agreement-17may01.htm>.

⁹ *Id.*, at para. 3.8.

¹⁰ *Id.*, at paras. 3.3-3.7. Note, however, that registrars are responsible for public access to Whois data only in the so-called "thin registry" TLDs, currently .com, .net, and .org. In the other so-called "thick registries," Whois service is the responsibility of the single registry operator for each registry.

¹¹ *Id.*, at para. 3.3. The information to be listed on the publicly accessible site is provided in para. 3.3.1.1 through 3.3.1.8. Whois data is also publicly available for free via a number of third-party portals, see, e.g., www.swhois.net.

¹² *Id.*, at para. 3.3.6.

¹³ *Id.*, at para. 3.7.7.1.

¹⁴ WIPO Mediation and Arbitration Center, Administrative Panel Decision, *National Hockey League And Lemieux Group Lp v. Domain For Sale*, Case No. D2001-1185.

the Russian Institute of Physics and Power Engineering in a town 100 kilometers south of Moscow.

- (2) The domain name www.kodakphotospot.com, which is listed by its owner as being for sale, does not provide an owner, administrative, or technical contact address.
- (3) For the domain name www.harleydavidsonmotorcompany.net, counsel investigating the ownership of the name found the telephone and fax numbers were listed as "+1.1111111111" in the Whois database.
- (4) Investigating the domain name www.amazonshopper.com, Amazon.com found that the domain name registrar had accepted the registration even with the registrant listing most of the contact information as "unknown." The telephone number for the administrative contact was listed as "+1.1234567891."

Presumably there is a means for addressing these flagrant violations of the RAA. Paragraph 3.7.8 of the RAA stipulates:

Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

Registrars also have the authority to cancel domain name registrations that are based on false contact data or whose registered owners do not make a timely response to an inquiry about allegedly false data. Paragraph 3.7.7.2 of the RAA stipulates:

A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure promptly to update information provided to Registrar, or its failure to respond for over fifteen calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.

Despite these provisions, many accredited registrars have been lax in investigating and cleaning up registrations with false Whois data. The dual problems of inaccurate Whois data and the failure on the part of domain name registrars to ensure reliable data has reached the point that some trademark owners no longer seek assistance from the domain name registrar. It is simply too time consuming and there is no guarantee of positive results. Instead, trademark owners are forced to hire private investigators to obtain the accurate contact data.

Trademark and copyright owners have repeatedly drawn ICANN's attention to the problems with respect to inaccurate Whois data. There is, however, only one reported instance in which ICANN has advised a domain name registrar that it was in violation of the RAA's Whois

provisions, specifically paragraph 3.7.8, and threatened to terminate the registrar's accreditation.¹⁴ Beyond this one case, we are not aware of any other time whereby ICANN has sought to enforce the Whois accuracy provisions of the RAA.

In addition to the problem of accuracy, trademark owners are also beginning to experience problems with respect to registrars granting accessibility to bulk Whois data. These problems were outlined in a May 1, 2003 letter from Jane Mutimear, president of the ICANN Intellectual Property Constituency (IPC), to ICANN's then-general counsel Louis Touton.

- A failure by domain name registrars to respond to requests for bulk Whois information.
- Deleting most of the information from the database before making it available under bulk Whois agreements; and
- Drafting of extremely restrictive, non-negotiable bulk Whois access contracts, which are so one-sided that they have served as a significant deterrent for third parties to enter into an agreement with registrars.¹⁵

The IPC letter added, "Denial of such access is a violation of the RAA, something that falls squarely within the purview of ICANN's enforcement responsibilities." To date, no one from ICANN has responded to this letter. In fact, we know of no action taken by ICANN to ensure that domain name registrars are complying with the bulk Whois requirements of the RAA.

Efforts to Improve Whois

There are efforts currently underway within ICANN that are designed to improve the collection and accuracy of Whois data and to address the ways that access to the data affects privacy and the proliferation of "spam." We assume these efforts would produce results more substantial than the limited number of minor changes that were recently implemented by ICANN, including the Whois data reminder policy (WDRP), which "calls for ICANN-accredited registrars to provide domain-name registrants with an annual listing of their Whois data and to remind registrants of the need to correct inaccurate or out-of-date information."¹⁶

Perhaps the most visible efforts to move forward on the Whois issue took place at the recent ICANN meeting in Montreal. A two-day workshop was held on the uses of Whois and possible new approaches to the structuring, accessibility, and use of the data. INTA expresses its gratitude to ICANN for holding the seminar and to the U.S. DOC for its role in organizing the event on behalf of the ICANN Governmental Advisory Committee (GAC). The presentations were informative and provided members of different constituencies with the opportunity to exchange ideas. We look forward to following up on those productive meetings.

¹⁴ Letter from Louis Touton to Bruce Beckwith, *Notice of Breach of ICANN Registrar Accreditation Agreement*, September 3, 2002, at <http://www.icann.org/correspondence/touton-letter-to-beckwith-03sep02.htm>.

¹⁵ Letter from Jane Mutimear (Intellectual Property Interests Constituency) to Louis Touton, May 1, 2003, at <http://www.icann.org/correspondence/mutimear-to-touton-01may03.htm>.

¹⁶ <http://www.icann.org/announcements/advisory-16jun03.htm>.

The follow up to the Montreal workshop, however, as well as the work of ICANN committees and task forces that are focusing on Whois, will take months, if not years to complete and then implement. In the meantime, the problems that we identified above, as well as others, continue to proliferate. Therefore, in the interim, ICANN itself must begin to take concrete steps to enforce the Whois and related provisions of the existing contracts, and must demonstrate a willingness to revoke the accreditation of domain name registrars that do not carry out their obligations. ICANN must dedicate more staff time and financial resources to this task and respond in a timely manner to complaints by the public concerning potential RAA violations. If it does not, ICANN not only risks the credibility that it has fought so hard to establish, but the stability of the DNS that is entrusted with, as well as becoming nothing more than a paper tiger in the eyes of domain name registrars.

The U.S. government, through the DOC, can play a critical role in ensuring that the provisions of the RAA are enforced by ICANN. One way this can be accomplished is by continuing to be a leader among the nations that participate in the GAC. INTA commends the work of former Under Secretary of Commerce Nancy Victory, DOC Associate Administrator Robyn Layton, and U.S. Patent and Trademark Office (USPTO) Attorney-Advisor Amy Cotton in protecting brand owner and consumer interests through their direct participation in the GAC.

The other way that the DOC can ensure that the RAA provisions are enforced is through the MOU. It is in the MOU that the DOC and ICANN agree upon those subjects to which ICANN will dedicate resources in the coming year. For example, in the present version of the MOU, ICANN agreed to "Continue its efforts to achieve stable agreements with [country code top-level domain] ccTLD operators."¹⁷ and "Continue the process of implementing new top level domains (TLDs)."¹⁸ Therefore, INTA requests that the DOC stipulate in the MOU, which is up for renewal later this month, that ICANN dedicate significant resources to enforcing its contracts with registrars and exercise its right under the RAA to take steps to revoke a registrar's accreditation if the registrar does not comply.

ccTLDs

Access to reliable Whois data and effective policies for resolving domain name disputes are also a concern in the country code top-level domain (ccTLD) space. The ccTLDs are the domains assigned to specific countries (e.g., .us for the United States, .uk for the United Kingdom, and .il for Israel). At present, there are over 240 ccTLDs in the world, and the number of ccTLD domain name registrations is growing rapidly. As of February 1, 2003, there are 19,158,364 registered domain names in ccTLDs, constituting 38.4% of the total number of domain names registered in the combined gTLD and ccTLD namespaces.¹⁹ The ccTLD for Germany, .de, is second only to .com in the total number of registrations with 6,117,000,²⁰ and .uk is the third largest TLD with 4,168,000 domain names.²¹

¹⁷ Amendment 5 to the MOU, *supra* note 2, at section II, amending V.C. of the MOU.

¹⁸ *Id.*

¹⁹ ICANN, Proposed Fiscal Year 2003-2004 Budget, Appendix 1, May 17, 2003, at <http://icann.org/financials/proposed-budget-17may03.htm>.

²⁰ *Id.* As of February 1, 2003, there are 23,239,000 domain names in .com.

²¹ *Id.*

At the recent ICANN meeting in Montreal, an agreement was reached concerning the formation of a ccTLD supporting organization, which would significantly assist ICANN in achieving agreements with ccTLD operators. INTA, through its participation in the IPC, supported the formation of the Country Code Name Supporting Organization (ccNSO) and compliments ICANN and the ccTLD administrators for coming to an agreement that will facilitate greater communication between them. We also acknowledge that ccTLD managers and ICANN have agreed that ccTLDs should have a mechanism “for making certain [registrant contact] data generally and publicly available (be it, for example, through Whois or nameservers).”²²

However, we are concerned that ccNSO mandate agreed to in Montreal is not sufficient in terms of improving the accuracy or the accessibility of Whois data in ccTLDs. It does not encourage the enforcement of Whois data policy in the ccTLD namespace. And, it fails to address the development of a cybersquatting dispute resolution policy for ccTLDs, something that would be akin to the UDRP that exists on the gTLD level.

The IPC had urged that ICANN play a direct role in the development of these policies. Uniformity of Whois and dispute resolution policies on the ccTLD level are just as important as they are on the gTLD level. It is essential to ensuring a safe, stable, and reliable online environment, particularly with ccTLD usage on the rise. ICANN should establish some broad-based policies for ccTLD administrators to implement regarding Whois and dispute resolution in their ccTLD. We suggest that the World Intellectual Property Organization’s *ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes*²³ be used as a guide for these policies.

Until such time as ICANN creates ccTLD policies regarding Whois and dispute resolution, INTA recommends that the U.S. government continue to insert into its bi-lateral trade agreements with other countries Whois and domain name dispute resolution language similar to that in the recently completed Chilean and Singaporean accords. INTA commends the U.S. government, particularly the DOC, USPTO, and U.S. Trade Representative, for inserting provisions that address the online concerns of trademark owners.

Conclusion

Thank you for the opportunity to submit a statement in connection with the subcommittee’s oversight of intellectual property safeguards on the Internet. INTA looks forward to working with the administration, this subcommittee, and our colleagues who are part of the Internet community to strengthen the safety and reliability of the DNS.

²² ICANN Bylaws, Annex C: The Scope of the ccNSO, The Core Functions, Data Entry Function (1)(b), at <http://www.icann.org/general/bylaws.htm>.

²³ <http://ecommerce.wipo.int/domains/ectlds/bestpractices/bestpractices.doc>.

Mr. SMITH. Thank you all again. We look forward to being in touch with you.

[Whereupon, at 3:14 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

DEPARTMENT OF COMMERCE STATEMENT REGARDING EXTENSION OF MEMORANDUM OF UNDERSTANDING WITH THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

Summary

The Memorandum of Understanding (MOU) between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) to transition management of the Internet domain name and numbering system (DNS) expires on September 30, 2003. The Department and ICANN have agreed to extend the term of the MOU for an additional three years, until September 30, 2006, and to amend the MOU in several important ways. These amendments are designed to ensure that ICANN develops into an independent, stable, and sustainable organization that is capable of meeting its responsibilities for the technical management of the DNS.

Background

The Department currently serves as the steward of critical elements of the DNS. ICANN is the private sector entity responsible for day-to-day management of the DNS. The Department continues to believe that the stability and security of this important global resource can best be achieved through privatization of and global participation in the technical management of the DNS. The Department supports the ongoing technical work of ICANN and its efforts to engage stakeholders in its decision-making processes. The Department especially desires to see ICANN evolve into an independent, stable, and sustainable organization that is well-equipped to weather a future crisis. ICANN has made progress toward this end, but in the Department's view, finalizing the future shape of ICANN is an urgent priority.

Last year, the Department and ICANN agreed to renew the MOU for a period of one year with a focus on improving stability and sustainability. ICANN undertook to clarify its mission and responsibilities; to ensure transparency and accountability in its processes and decision making; to increase its responsiveness to Internet stakeholders; to develop an effective advisory role for governments; and to ensure adequate and stable financial and personnel resources to carry out its mission and responsibilities.

In pursuing these tasks, ICANN made important strides towards developing into a more stable, transparent, and responsive organization. ICANN completed a comprehensive reform effort that resulted in major structural adjustments and refinements to its decision-making processes to permit greater transparency and responsiveness to all Internet stakeholders. In addition, the corporation hired a new Chief Executive Officer having both management expertise and experience in dealing with this unique organization. It also implemented a new nominating process to attract qualified, committed, and internationally representative members on its Board of Directors. ICANN recently appointed eight new Board members with impressive credentials and relevant experience. Moreover, the ICANN Governmental Advisory Committee (GAC), of which the United States is an active participant, has also evolved into a more effective organization. The GAC has established liaisons to each of the ICANN supporting organizations to encourage communications between the GAC and these constituent groups.

Modifications to the MOU and Departmental Expectations

The Department welcomes ICANN's achievements over the past year. Yet, as both the Department and ICANN recognize, much work remains for ICANN to evolve into an independent, stable, and sustainable DNS management organization. The Department also recognizes that the term of the MOU should provide sufficient time for this work to be accomplished. Accordingly, the Department and ICANN have agreed to a three-year extension of the MOU and the incorporation of milestones. The Department expects that this extension will be sufficient for ICANN to complete the tasks remaining under the MOU. It will allow ICANN, under its new leadership, to implement the structural and organizational changes that have been adopted in the past year. The extension should also permit ICANN to stabilize and to secure the necessary financial and personnel resources critical to long-term sustainability of the organization. In addition, it should afford ICANN ample time to provide opportunities for enhanced cooperation from Internet stakeholders.

To ensure steady progress throughout the renewed MOU term, the Department and ICANN agreed to the incorporation of numerous specific milestones into the agreement. These milestones are intended to ensure ICANN is a sufficiently stable, transparent, representative, efficient, and sustainable management organization capable of handling the important DNS tasks well into the future. These milestones cover the following areas:

Strategic Plan - - By December 31, 2003, ICANN will develop a strategic plan that sets forth its goals for securing long-term sustainability of critical DNS management responsibilities, including the necessary corporate structure and financial and personnel resources necessary to meet such responsibilities. The amendment further provides for a variety of measurable objectives and corresponding milestones for achieving those objectives. For example, ICANN will review and augment its corporate compliance program, including a system for auditing material contracts for compliance by all parties, and will implement any recommendations resulting from this review by June 30, 2004.

Corporate Structure - - By March 31, 2004, building on ICANN's recent efforts to re-examine its mission, structure, and processes for their efficacy and appropriateness in light of the needs of the evolving DNS, ICANN will collaborate with the Department to ensure that ICANN's corporate organizational documents optimally support the policy goal of privatization of the technical management of the DNS.

Contingency Plan - - By June 30, 2004, ICANN will develop a contingency plan to ensure continuity of operations in the event the corporation incurs a severe disruption of operations, or the threat thereof, by reason of its bankruptcy, corporate dissolution, a natural disaster, or other financial, physical or operational event. In conjunction with its efforts in this regard, ICANN will work collaboratively with the Department to ensure that such plan reflects the international nature of the DNS.

Root Server System Security - - The root server system forms the critical infrastructure of the DNS by linking domain names to the corresponding numerical addresses. ICANN will formalize

its relationship with the root server system operators to enhance the security of the root server system.

Allocation of Numbering Resources - - ICANN will enter into agreements with Regional Internet Registries, which are responsible for allocating numbering resources within their respective geographic regions.

Transparency and Accountability - - ICANN will continue to develop, test, and implement processes and procedures to improve transparency, efficiency, and timeliness in the consideration and adoption of policies related to technical management of the DNS. In conjunction with this effort, ICANN will take into account the need to accommodate innovation in the provision of DNS services. In addition, ICANN will continue to develop, test, and implement accountability mechanisms.

Country Code Top Level Domains - - ICANN will continue its efforts to achieve agreements with country code top level domain operators.

New Top Level Domains - - ICANN will develop, by September 30, 2004, and will implement by December 31, 2004, an appropriate long-term strategy for selecting new top level domains.

WHOIS Database - - ICANN will assess the operation of the WHOIS databases and implement measures to secure improved accuracy of WHOIS data. In addition, by March 31, 2004, and annually thereafter, ICANN will publish a report providing statistical and narrative information on the InterNIC WHOIS Data Problem Reports system. By November 30, 2004, and annually thereafter, ICANN will publish a report providing statistical and narrative information on the implementation of the ICANN WHOIS Data Reminder Policy. Both reports will contain an evaluation of the impact of these policies on improved accuracy of WHOIS data.

Outreach - - ICANN will continue to develop, test and implement appropriate mechanisms that foster informed participation in ICANN by the global Internet community, such as providing educational services and fostering information sharing for constituents and promoting best practices among industry segments.

Conclusion

While numerous issues and substantial challenges confront ICANN, the organization has made notable progress toward achieving the goals of the MOU in the start-up phase of its existence. The Department and ICANN both now seek to complete the transition of DNS management to the private sector. Thus, in its next phase, it is essential that ICANN effectively address mission, operational, and organizational challenges to its long-term success. While the Department stands ready to continue its stewardship of critical DNS elements during the transition period, it is incumbent upon governments, private sector companies, and users across the globe to work towards establishing mechanisms for managing the DNS that are sustainable over the long term. To this end, the Department remains committed to working diligently with ICANN and Internet stakeholders to assist ICANN in its evolution and to preserve and enhance this global resource.

**MEMORANDUM OF UNDERSTANDING BETWEEN
THE U.S. DEPARTMENT OF COMMERCE AND
THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS**

Amendment 6

WHEREAS, the U.S. Government supports the policy of privatizing the technical management of the Internet and its underlying domain name system (DNS) now performed by or on behalf of the U.S. Government or by third parties under arrangements or agreements with the U.S. Government;

WHEREAS, the U.S. Government effects such privatization by entering into agreement with and seeking international support for a not-for-profit corporation formed by private sector Internet stakeholders to administer DNS policy;

WHEREAS, on November 25, 1998, the U.S. Department of Commerce (Department) on behalf of the U.S. Government entered into a Memorandum of Understanding (Agreement) with the Internet Corporation for Assigned Names and Numbers (ICANN), a private sector, not-for-profit corporation, for the purpose of the joint development of the mechanisms, methods, and procedures necessary to effect the transition of DNS management to the private sector;

WHEREAS, the Agreement contemplated that the Parties would collaborate on the DNS Project, in which the Parties would jointly design, develop, and test the mechanisms, methods, and procedures to carry out the following DNS management functions:

- a. Establishment of policy for and direction of the allocation of IP number blocks;
- b. Oversight of the operation of the authoritative root server system;
- c. Oversight of the policy for determining the circumstances under which new top level domains would be added to the root system;
- d. Coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet, and
- e. Other activities necessary to coordinate the specified DNS management functions, as agreed by the Parties;

WHEREAS, work to be performed under the Agreement was intended to demonstrate that management responsibility for the DNS could be performed by ICANN;

WHEREAS, the Agreement has been amended five times to refine the work to be performed and to extend the term of the Agreement, such term currently to expire on September 30, 2003;

WHEREAS, ICANN has made significant progress over the past year towards achieving the tasks set forth in Amendment 5 of the MOU, including refining its mission and restructuring its supporting groups and advisory committees; implementing new constituency driven policy-development processes; establishing a country code Names Supporting Organization; establishing an at-large advisory committee and regional at-large organizations; creating liaisons between the Governmental Advisory Committee (GAC) and all ICANN supporting organizations and advisory committees; establishing a new procedure for board nominations; and restructuring staff under the leadership of a new Chief Executive Officer (CEO) to respond to ICANN's technical policy, DNS management, and financial responsibilities;

NOW THEREFORE, in recognition of ICANN's progress in achieving the tasks and goals set forth in the Agreement and of its on-going work on reforming its structure and operations as described in the *Eighth Status Report to the Department*, dated August 1, 2003, the Parties hereby agree as follows:

- I. The Department reaffirms its policy goal of privatizing the technical management of the DNS in a manner that promotes stability and security, competition, coordination, and representation. Consistent with this objective and in furtherance of the DNS Project, the Parties agree to strike V.B. in its entirety and to substitute the following:
 - B. Department. The Department agrees to perform the following activities and provide the following resources in support of the DNS Project:
 1. Provide expertise and advice on DNS management functions.
 2. Provide expertise and advice on methods and administrative procedures for conducting open, public proceedings concerning policies and procedures that address the technical management of the DNS.
 3. Identify with ICANN the necessary software, databases, know-how, other equipment, and intellectual property necessary to design, to develop, and to test methods and procedures of the DNS Project.
 4. Participate, as necessary, in the design, development, and testing of the methods and procedures of the DNS Project to ensure continuity, including coordination between ICANN and VeriSign, Inc.
 5. Collaborate with ICANN on operational procedures for the root name server system, including formalization of relationships under which root name servers throughout the world are operated and continuing to promote best practices used by the root system operators.
 6. Continue to consult with the managers of root name servers operated by the U.S. Government and with other responsible United States Government agencies with respect to operational and security matters of such root name servers and recommendations for improvements in those matters.

7. Work collaboratively within ICANN's GAC to encourage the creation of stable agreements between ICANN and the organizations and entities operating country code Top Level Domains (ccTLDs).
 8. Work collaboratively within ICANN to encourage the creation of stable agreements between ICANN and the Regional Internet Registries (RIRs).
 9. Consult with the international community on aspects of the DNS Project.
 10. Provide general oversight of activities conducted pursuant to this Agreement.
 11. Maintain oversight of the technical management of the DNS functions currently performed either directly by, or subject to agreements with, the U.S. Government, until such time as further agreement(s) are arranged as necessary for ICANN to undertake management of specific DNS technical management functions.
 12. Consult with foreign governments to promote increased and more effective governmental participation in the GAC.
 13. In conjunction with ICANN's efforts to develop a corporate contingency plan as described in Section II.C.11 of this Amendment, work collaboratively with ICANN to ensure that such plan reflects the international nature of the DNS.
 14. Building on ICANN's recent efforts to reexamine its mission, structure, and processes for their efficacy and appropriateness in light of the needs of the evolving DNS, collaborate with ICANN to ensure that its corporate organizational documents optimally support the policy goal of privatization of the technical management of the DNS.
- II. ICANN reaffirms its commitment to maintaining security and stability in the technical management of the DNS, and to perform as an organization founded on the principles of competition, bottom up coordination, and representation. Consistent with these objectives and in furtherance of the DNS Project, the Parties agree to strike V.C. in its entirety from Amendment 5 to the MOU and to substitute the following:
- C. ICANN, ICANN agrees to perform the following activities and provide the following resources in support of the DNS Project, in conformity with the ICANN Board-approved mission and core values and in furtherance of its ongoing reform efforts:
1. Continue to provide expertise and advice on private sector functions related to technical management of the DNS.
 2. Work collaboratively on a global and local level to pursue formal legal agreements with the RIRs, and to achieve stable relationships that allow them to continue their technical work, while incorporating their policy-making activities into the ICANN process.

3. Continue to develop, to test, and to implement processes and procedures to improve transparency, efficiency, and timeliness in the consideration and adoption of policies related to technical management of the DNS. In conjunction with its efforts in this regard, ICANN shall take into account the need to accommodate innovation in the provision of DNS services.
4. Continue to develop, to test, and to implement accountability mechanisms to address claims by members of the Internet community that they have been adversely affected by decisions in conflict with ICANN's by-laws, contractual obligations, or otherwise treated unfairly in the context of ICANN processes.
5. Collaborate with the Department on operational procedures for the root name server system, including formalization of relationships under which root name servers throughout the world are operated and continuing to promote best practices used by the root system operators.
6. Continue to consult with the managers of root name servers and other appropriate experts with respect to operational and security matters relating to the secure and stable operation of the domain name and numbering system in order to develop and implement recommendations for improvements in those matters, including ICANN's operation of the authoritative root, under appropriate terms and conditions.
7. Continue its efforts to achieve stable agreements with ccTLD operators that address, among other things, issues affecting the stable and secure operation of the DNS, including: delegation and redelegation of ccTLDs; allocation of global and local policy-formulation responsibility; and the relationship between a ccTLD operator and its relevant government or public authority. Such efforts shall include activities to encourage greater dialogue between ccTLD operators and their respective governmental authority.
8. Continue the process of implementing new top level domains (TLDs), which process shall include consideration and evaluation of:
 - a. The potential impact of new TLDs on the Internet root server system and Internet stability;
 - b. The creation and implementation of selection criteria for new and existing TLD registries, including public explanation of the process, selection criteria, and the rationale for selection decisions;
 - c. Potential consumer benefits/costs associated with establishing a competitive environment for TLD registries; and,
 - d. Recommendations from expert advisory panels, bodies, agencies, or organizations regarding economic, competition, trademark, and intellectual property issues

Define and implement a predictable strategy for selecting new TLDs using straightforward, transparent, and objective procedures that preserve the stability of the Internet (strategy development to be completed by September 30, 2004 and implementation to commence by December 31, 2004).

9. Continue to develop, to test, and to implement appropriate mechanisms that foster informed participation in ICANN by the global Internet community, such as providing educational services and fostering information sharing for constituents and promoting best practices among industry segments.
10. Continue to assess the operation of WHOIS databases and to implement measures to secure improved accuracy of WHOIS data. In this regard,
 - a. ICANN shall publish a report no later than March 31, 2004, and annually thereafter, providing statistical and narrative information on community experiences with the InterNIC WHOIS Data Problem Reports system. The report shall include statistics on the number of WHOIS data inaccuracies reported to date, the number of unique domain names with reported inaccuracies, and registrar handling of the submitted reports. The narrative information shall include an evaluation of the impact of the WHOIS Data Problem Reports system on improved accuracy of WHOIS data.
 - b. ICANN shall publish a report no later than November 30, 2004, and annually thereafter, providing statistical and narrative information on the implementation of the ICANN WHOIS Data Reminder Policy. The report shall include statistics on registrar compliance with the policy and information obtained regarding results of the implementation of the WHOIS Data Reminder Policy. The narrative information shall include implementation status, information on problems encountered, and an evaluation of the impact of the WHOIS Data Reminder Policy on improved accuracy of WHOIS data.
11. By June 30, 2004, ICANN shall develop a contingency plan to ensure continuity of operations in the event the corporation incurs a severe disruption of operations, or the threat thereof, by reason of its bankruptcy, corporate dissolution, a natural disaster, or other financial, physical or operational event. In conjunction with its efforts in this regard, ICANN shall work collaboratively with the Department to ensure that such plan reflects the international nature of the DNS.
12. Collaborate on other activities as appropriate to fulfill the purpose of this Agreement, as agreed by the Parties.
13. Building on ICANN's recent efforts to reexamine its mission, structure, and processes for their efficacy and appropriateness in light of the needs of the evolving DNS, collaborate with the Department to ensure that ICANN's corporate organizational documents optimally support the policy goal of privatization of the technical management of the DNS (collaboration to be completed by March 31, 2004).

14. By December 31, 2003, develop a strategic plan that sets forth ICANN's goals for securing long-term sustainability of its critical domain name and numbering system management responsibilities, including the necessary corporate structure and financial and personnel resources to meet such responsibilities. Such plan should address, among other areas, the following items, and should include measurable objectives and milestones for achievement of such objectives:
 - a. Conduct a review of corporate administrative structure and personnel requirements, including executive compensation and management succession plan (implementation of any recommendations resulting from review to be completed by March 31, 2004);
 - b. Conduct a review of internal mechanisms that promote and ensure Board of Directors, executive management, and staff corporate responsibility (implementation of any recommendations resulting from review to be completed by March 31, 2004);
 - c. Develop and implement a financial strategy that explores options for securing more predictable and sustainable sources of revenue (strategy development to be completed by June 30, 2004 and implementation to commence by December 31, 2004);
 - d. Review and augment its corporate compliance program, including its system for auditing material contracts for compliance by all parties to such agreements (implementation of any recommendations resulting from review to be completed by June 30, 2004);
 - e. Develop a collaborative program with private and intergovernmental parties to conduct outreach to governments and local Internet communities in targeted regions, including key constituencies (commence program operation by December 31, 2004);
 - f. Develop and implement an appropriate and effective strategy for multi-lingual communications (commence strategy implementation by December 31, 2004); and
 - g. Conduct review of system-wide efforts to automate operational processes (implementation of any recommendations resulting from review to be completed by June 30, 2005).
15. Provide a status report to the Department on its progress towards the completion of its tasks under this Agreement, including implementation of ICANN's strategic plan, on or before five (5) business days following the end of each six-month period that this Agreement is in effect.

III. Strike Section VII of the Agreement and replace it, in its entirety, with:

- A. In furtherance of the objective of this Agreement, to support the completion of the transition of DNS management to the private sector, the Department and ICANN will hold regular meetings between senior Departmental officials and ICANN senior management and leadership to assess progress.
- B. This Agreement will become effective upon signature of ICANN and the Department. This Agreement will terminate on September 30, 2006. This Agreement may not be amended except upon the mutual written agreement of the Parties. Either Party may terminate this Agreement by providing one hundred twenty (120) days written notice to the other Party. If this Agreement is terminated, each Party shall be solely responsible for the payment of any expenses it has incurred. This Agreement is subject to the availability of funds.

IV. Except as specifically modified by this Amendment 6, the terms and conditions of the Agreement, as previously amended, remain unchanged.

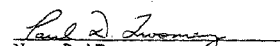
FOR THE NATIONAL
TELECOMMUNICATIONS AND
INFORMATION ADMINISTRATION:


Name: Michael D. Gallagher

Title: Acting Assistant Secretary for
Communications and Information

Date: September 16, 2003

FOR THE INTERNET CORPORATION
FOR ASSIGNED NAMES AND
NUMBERS:


Name: Paul Twomey

Title: President and CEO

Date: September 16, 2003

PREPARED STATEMENT OF THE HONORABLE ROBERT WEXLER, A REPRESENTATIVE IN
CONGRESS FROM THE STATE OF FLORIDA

Mr. Chairman:

I want to thank you for holding this important hearing today; however, I am deeply concerned with an issue related to today's hearing.

At a recent Senate hearing in the Commerce, Science & Transportation Committee, Senator Cantwell got assurance from the Commerce Department, specifically from the departing head of the NTIA, that the Commerce Department believes it is authorized to review and make a decision on approving ICANN's proposal to grant VeriSign a contract that will provide exclusive control over the backordering of domain names. This proposal would effectively end the competition that exists today among some 100 firms engaged in this industry, including some in my state of Florida.

As the Department of Commerce moves forward in its dealings with ICANN, I feel that the Judiciary will require an assurance that the Department will review the impact of ICANN's proposed exclusive contract concerning the backordering of domain names on competition, particularly as it affects small businesses and consumers. Additional scrutiny of this matter by the Judiciary is warranted, particularly given that despite the official assurance the Department of Commerce gave to Senator Cantwell in July and despite any official approval on such a measure from the Department of Commerce or any evaluation by the Department on the measure's impact on the consumer or the dozens of small businesses now providing this service, this proposed exclusive backordering service is already being advertised on the Internet, saying that it will take effect in October. Mr. Chairman, I hope you will join me in ensuring that these questions be adequately resolved before the Department of Commerce finalizes its Memorandum of Understanding with ICANN.

September 4, 2003

The Honorable Lamar S. Smith
House of Representatives
Washington, DC 20515

The Honorable Howard L. Berman
House of Representatives
Washington, DC 20515



1004 E Street, NW Suite 1100
Washington, DC 20006
202.637.8900
fax 202.637.0964
<http://www.cdt.org>

Dear Chairman Smith and Representative Berman:

In conjunction with the Subcommittee's hearing on Whois accuracy, we write to urge the Subcommittee to consider the real privacy questions raised for people who register domain names and must put sensitive personal information in the publicly available Whois database. There are valuable technical, consumer protection and enforcement benefits from Whois, but CDT believes a balanced approach can be achieved that preserves enforcement while protecting personal privacy.

The Whois database—a public listing of contact information for millions of domain name registrants—does create substantial public benefits. Originally designed to allow contact in the case of a technical problem, the database is now also used by law enforcement, consumer protection agencies, and private groups including intellectual property holders.

While uncontroversial for commercial registrations, Whois may require that individual Internet users, when they register domain names, make their names, home addresses, home phone numbers, and home e-mail addresses available to the world. Such potentially sensitive personal information, released publicly, can be abused for purposes ranging from unwelcome marketing to identity theft, fraud, stalking, and other criminal activities.

The current Whois regime is on a collision course with public sensitivities and international law. In an era of concern about identity theft and online security, it is unwise to require millions of individual registrants to place their home phone numbers, home addresses, and personal email accounts into a publicly available database that places no restrictions on the use of that data. Such an approach also violates the privacy laws of some nations. Absent safeguards to protect privacy and security, law-abiding people will continue to place inaccurate data in the Whois database. The best way to achieve accuracy in the Whois database will be to guarantee registrants privacy and security for their information.

There are solutions to these problems that would provide added privacy protections for Whois data while preserving its technical and enforcement benefits. Proposals include creating a "tiered access" system for viewing Whois data, providing notice to users when their data is viewed, and creating "audit trails" that could expose abuse or misuse of the database.

CIDT believes a balance can be struck that protects privacy and allows reasonable access to data for important public purposes. We look forward to working with the Subcommittee and the ICANN community to craft such a balanced approach.

Respectfully,

A handwritten signature in black ink, appearing to read 'A. Davidson', followed by a horizontal line.

Alan Davidson
Center for Democracy and Technology
1634 Eye St. NW
Suite 1100
202-637-9800

September 11, 2003

Chairman Lamar C. Smith
 Ranking Member Howard L. Berman
 Subcommittee on Courts, the Internet and Intellectual Property
 Committee on the Judiciary
 United States House of Representatives

Dear Chairman Smith and Congressman Berman:

As a group of ICANN accredited registrars representing a majority of global top level domain (gTLD) registrations, we respectfully submit information for the record of the Hearing on the Internet and the WHOIS Database that you held on September 4, 2003.

The Committee is to be commended for holding a timely hearing on an issue of importance to the ICANN community and to the interests of U.S. and worldwide consumers and businesses. We take this opportunity to submit the following remarks that should serve to supplement the record and address certain concerns raised by Committee members during the hearing.

Most active registrars take their obligations in the ICANN agreements very seriously. Likewise, we take seriously our relationship with our customers and recognize their concerns regarding the privacy of their personal data and the abuse of WHOIS data that leads to spam and other undesirable practices that degrade the Internet experience. In any industry, there are actors whose business practices do not live up to the community standard. However, the general practices among accredited registrars demonstrate compliance with ICANN obligations as well as sensitivity to consumer concerns.

Contractual obligations in the standard ICANN Registrar Accreditation Agreement (RAA) place the responsibility of providing accurate WHOIS data squarely on registrants. The RAA identifies the specific data that registrars are obligated to collect from registrants during the domain name registration process. While registrants bear the primary burden of providing accurate WHOIS data, ICANN nevertheless imposes certain requirements on registrars that foster the provision and maintenance of accurate WHOIS data.

First, upon receipt of a complaint concerning inaccurate WHOIS data, registrars are required to contact the registrant in question and notify the registrant that a complaint about inaccurate WHOIS data on their domain name registration[s] has been received. Registrars provide the registrant with a brief period of time to confirm the accuracy of the WHOIS data or to make any necessary corrections. Failure to do so can result in the cancellation of the domain name registration. The seriousness of this sanction underscores the importance registrars and ICANN place on the accuracy of WHOIS data.

Second, ICANN recently adopted the Whois Data Reminder Policy (WDRP). The WDRP policy, which must be implemented by registrars no later than October 31, 2003 (with the exception of newly accredited registrars who have a longer period for compliance), requires registrars to remind their customers on an annual basis of the obligation to provide and maintain accurate

WHOIS data. The WDRP obligation requires registrars to present each registrant with a copy of the WHOIS record for his or her registration[s] along with an explicit warning that the provision of false WHOIS data can be grounds for cancellation of the registration[s]. Thus, the newly adopted WDRP will serve as an important tool in fostering the accuracy of WHOIS data.

Third, registrants can, and do, update their WHOIS data in the course of managing their account over time. Registrars typically provide their customers with the ability to update or change their WHOIS data by accessing the registrar's online storefront. Notices such as the WDRP will have the effect of driving registrants to their respective registrars' online websites on a more regular basis.

It must be noted that, even given the above examples, instances of inaccurate WHOIS data will continue to occur. Frankly stated, individual bad actors who do not wish to provide accurate data at the time of domain name registration will continue to provide inaccurate data despite the best efforts of registrars and ICANN alike. Additionally, registrars hear complaints from legitimate registrants regarding the lack of privacy in the WHOIS database. In order to avoid spam and fraud, and to generally preserve their privacy, many registrants - as well as various legal privacy regimes - demand the screening of personal contact data, such as phone numbers and email addresses. Such concerns about the lack of privacy can also result in the provision of inaccurate WHOIS data by registrants. Some registrars have responded to consumer demand for privacy protection by instituting programs to guard against the harvesting (bulk copying) of WHOIS data by spammers and by providing registrants with the ability to subscribe to "private registrations" which allow registrants to enter alternate contact data (albeit valid and reliable) in the WHOIS record. Even in the case of private registrations, registrars cooperate with legitimate interests such as law enforcement and intellectual property holders to reveal the registrant's actual personal data in appropriate circumstances.

As demonstrated by the foregoing, registrars undertake significant effort to facilitate accurate WHOIS data and to provide registrants with some level of protection against harm that can arise from the public display of their personal data. While the WDRP notice requirement is another tool to ensure greater accuracy of WHOIS data, requirements of this nature are not without cost. Communications, data processing and personnel costs of compliance are significant, even more so for registrars having sizeable customer bases. Designing and implementing procedures, programs and systems that run in an automated fashion is not a trivial exercise for an industry that operates on very thin margins. Additional requirements would impose significant unanticipated costs, such as drafting new legal agreements, designing software systems, implementing new processes and increased customer service support.

Despite registrars' best efforts, it must be recognized that the verification of registrant data is subject to real world limitations. Verification of personal contact data in the U.S. alone is an uncertain task. Given the fact that registrants for gTLD names reside in every region of the world, it is not a stretch to say that it is impossible to verify every registrant's data prior to completing registration or to confirm that the registrant actually resides at a proffered address or is the subscriber to a proffered telephone number. One telling example encountered by a registrar concerns a registrant's address that was listed as "120 meters past McDonald's on Rue Flat

Road.” While this may appear to be facially false data, the registrar noted that a hotel on the same street stated its address as, “240 meters past McDonald’s.” Should the registrant in this example re-iterate said address in response to a complaint about inaccurate WHOIS data, would the registrant have a basis to cancel the registration in question?

In conclusion, registrars take their obligations to their customers and to ICANN very seriously. They implement a variety of methods in an effort to maintain accurate Whois data and will continue to do so. We would appreciate the inclusion of this letter in the record of the hearing. Please do not hesitate to call on us for any questions that you might have.

Sincere Regards,

X

Brian Cute
Director of Policy
Network Solutions, Inc.

X

Elana Broitman
Director of Policy
Register.com

X

Tom D’Alleva
Vice President
Bulk Register

X

Paul Stahura
President
eNom



1775 Wiehle Avenue
Suite 102A
Reston, VA 20190
+1-703-464-7005
+1-703-464-7006 fax
www.pir.org

BOARD OF DIRECTORS

David W. Maher (USA)
Chairman
Alan Levin (Africa)
Treasurer
Andy Linton (Australasia)
Secretary
Gerry Barañano (USA)
Frode Gressen (Europe)
Lawrence H. Landweber (USA)
Marc Rotenberg (USA)
Lynn St. Amour
(USA and Europe)
Ex-officio ISOC liaison
Edward G. Viltz
President and CEO

The Honorable Howard L. Berman
Subcommittee on Courts, the Internet, and Intellectual Property
House Judiciary Committee
Rayburn House Office Building
Room 2221
Washington, DC 20515
September 16, 2003

Dear Congressmen Berman,

We write to you, on behalf of the Public Interest Registry, (PIR), regarding Internet privacy and the September 4th hearing on WHOIS. PIR appreciates the interest that the committee has shown in the operation of WHOIS, an important database for the management of the Internet. At the same time, we are concerned that the committee has failed to consider the significant privacy issues surrounding the WHOIS database or the need to ensure that the goal of accuracy and privacy safeguards are pursued simultaneously. As one of the largest Internet registries in the world, PIR has a particular interest in ensuring that the policies developed for the WHOIS database respect the interests of individuals who register Internet domains.

The Public Interest Registry the not-for-profit corporation that manages the .ORG registry, is responsible for the nearly 3 million registrants in the .ORG domain. PIR is dedicated to providing an open, responsible, and truly global approach for the .ORG community. PIR was created by the Internet Society (ISOC), a professional membership society that provides leadership in addressing issues that confront the future of the Internet. ISOC is the organizational home for the groups responsible for Internet infrastructure standards. Together PIR and ISOC are working to promote the continued growth and development of the Internet.

All users of domain names have a justified and reasonable expectation of privacy, and there are many users, particularly in the noncommercial world, who have legitimate reasons to conceal their identities or to register domain names anonymously. Unfortunately, there are also some domain name registrants who use the Internet to conduct fraud or whose use violates intellectual property rights of other users. PIR believes that a sensible policy for WHOIS must consider both



Serving the Public Interest

Public
Interest
Registry

1775 Wiehle Avenue
Suite 102A
Reston, VA 20190
+1-703-464-7005
+1-703-464-7006 fax
SM www.pir.org

Page 2

legitimate privacy expectations for domain registrants and some form of access to WHOIS data to deal with fraudulent and improper use of domain names.

In these comments, PIR is responding to the statements of various participants in the September 4 oversight hearing on "Internet Domain Name Fraud - the U.S. Government's Role in Ensuring Public Access to Accurate WHOIS Data". While accurate data may be preferable to inaccurate, PIR believes that the Subcommittee has failed to consider the critical issues of privacy and data protection.

The noncommercial community served by PIR would be especially disadvantaged by a policy that fails to protect adequately the privacy of Internet registrants. WHOIS data currently consists of contact information (including address information on registrants, administrative contacts, and technical contacts). Domain registrants include businesses; individuals; media organizations; non-profit groups; public interest organizations; political organization; religious organizations; support groups; and so on. These domain name registrants may share their services, organizations, ideas, views, and activities by way of websites, email, newsgroups, and other Internet media. While some domain name registrants may use the Internet to conduct fraud, the vast majority does not, and many registrants have legitimate reasons to conceal their identities or to register domain names anonymously. In fact, requiring detailed personal information to be publicly available almost certainly facilitates fraud. WHOIS data is globally, publicly accessible. Everyone with Internet access, including those with bad motives as well as those with good motives, has access to WHOIS data.

It is critical that the Subcommittee understand the important privacy issues surrounding WHOIS as well as the risk that the widespread dissemination of personal information could actually exacerbate the problem of Internet-based fraud.

First, compelling the disclosure of personal information, even information related to domain registration, poses dangers to freedom of expression and privacy on the Internet. Domain name registrants - and particularly the noncommercial users of the .ORG domain - may not wish to make public the information furnished by them to registrars.

Some of them may have legitimate reasons to conceal their actual identities or to register domain names anonymously. For example, there are political, cultural and religious groups around the world that rely on anonymous access to the Internet to publish their messages. In order to avoid persecution, anonymity may be critical in this respect. It is important to note that anonymizing proxy servers are not an adequate alternative.

Second, anyone with Internet access -- including spammers, stalkers, scam artists, identity thieves, and others with no legitimate interests, has access to WHOIS data. It is well known that access to personal information online contributes to frauds such as identity theft. The Federal Trade Commission (FTC) report "National and State Trends in Identity Theft" found that identity theft is the number one consumer complaint and constitutes 43% of all complaints in the agency's complaint database. The FTC advises consumers to protect themselves from identity theft and generally from Internet-related frauds by not disclosing personally identifiable information. In all cases, when consumers choose to disclose such information, they should know who is collecting it, why it is being collected, and how it is going to be used. The mandatory publication of WHOIS data is contrary to this sound advice. The domain name registrant has no control over or information about the uses of WHOIS data.

Third, the .ORG community is international in scope, and PIR seeks to respect international views on privacy and data protection. Policies pursued in the United States that fail to respect privacy concerns established in law elsewhere in the world will disadvantage our organization and lead Internet users to register with others outside the United States that will provide stronger privacy safeguards.

We urge the Subcommittee to consider our views and the views of others on Internet privacy before any further action is taken on the WHOIS issue. At a minimum, PIR believes it essential that the purposes of the collection and publication of personal data of domain name holders be specified. The amount of data collected and made publicly available in the course of the registration of a domain name should be limited to what is essential to fulfill the purposes specified. Any secondary use incompatible with the original purpose specified should require the individual's informed consent. Such a policy would not



1775 Wiehle Avenue
Suite 102A
Reston, VA 20190
+1-703-464-7005
+1-703-464-7006 fax
www.pir.org

Page 4

frustrate legitimate criminal investigations or copyright investigations. It would help ensure base level privacy safeguards and reduce the risk that the widespread availability of personal information will lead to greater fraud, possibly putting millions of Internet users at risk.

We ask that our comments be included in the hearing record for the September 4th hearing. We would also appreciate the opportunity to meet with Members of the Subcommittee in the near future regarding these critical issues.

We appreciate your consideration of our views.

Warmest Regards,

David W. Maher
Chairman of the Board

cc: Mr. Michael D. Gallagher, Acting NTIA Administrator
Dr. Paul Twomey, ICANN President and CEO