# FRAUDULENT ONLINE IDENTITY SANCTIONS ACT

## HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

ON

**H.R. 3754**

FEBRUARY 4, 2004

**Serial No. 63**

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
91–605 PDF WASHINGTON : 2004

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
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

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
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
JOHN R. CARTER, Texas

HOWARD L. BERMAN, California
JOHN CONYERS, JR., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

BLAINE MERRITT, *Chief Counsel*
DAVID WHITNEY, *Counsel*
MELISSA L. MCDONALD, *Full Committee Counsel*
ALEC FRENCH, *Minority Counsel*

# CONTENTS

FEBRUARY 4, 2004

## OPENING STATEMENT



## WITNESSES



## APPENDIX

### MATERIAL SUBMITTED FOR THE HEARING RECORD

# FRAUDULENT ONLINE IDENTITY SANCTIONS ACT

**WEDNESDAY, FEBRUARY 4, 2004**

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

The Subcommittee met, pursuant to notice, at 10:09 a.m., in Room 2141, Rayburn House Office Building, Hon. Lamar S. Smith (Chair of the Subcommittee) presiding.

Mr. SMITH. The Subcommittee on Courts, the Internet, and Intellectual Property will come to order. I am going to recognize myself for an opening statement, then the Ranking Member, Mr. Berman, and without objection, other Members' opening statements will be made a part of the record.

Today's hearing is on H.R. 3754, the "Fraudulent Online Identity Sanctions Act." There are two overriding characteristics of this bill which the Ranking Member, Mr. Berman, and I have introduced. First, we target those who register false domain name contact information in furtherance of a Federal criminal offense or in violation of Federal copyright or trademark law. Second, we ensure that these individuals face more severe civil and criminal penalties for their regrettable conduct.

Five months ago, this Subcommittee conducted an oversight hearing entitled, "Internet Domain Name Fraud: The U.S. Government's Role in Ensuring Public Access to Accurate Whois Data." At that time, the Department of Commerce was considering whether and under what terms to renew its agreement with the Internet Corporation for Assigned Names and Numbers, ICANN.

As a result of the testimony received that day and the attention focused on the U.S. Government's negotiations with ICANN, the Commerce Department required ICANN for the first time to implement a series of Whois specific reports and improvements. I am disappointed to say that the early signs from ICANN are not encouraging.

It is beyond dispute that the public needs and deserves access to accurate data on domain name registrants. Whois was created to serve precisely this role. Whois data is relied upon by a wide variety of users, but is particularly important to those in the IP community. Copyright owners use it to identify pirate sites that operate on the Internet. Trademark owners use it to resolve cybersquatting disputes and to track down owners of websites that

offer counterfeit goods or otherwise infringe upon intellectual property rights.

Parents and law enforcement officers rely on Whois data to protect our children from online threats. Officials have publicly stated the database is the first step in most web-based child pornography and exploitation cases. Consumers and businesses rely on Whois to identify the owners of websites in order to protect confidential information, such as credit card numbers.

Late last month, the Federal Trade Commission released its 2003 consumer sentinel report on trends and fraud in identity theft. The report revealed that Internet-based scams were second only to identity theft as the top fraud complaint reported to the Government. In 2003, Internet-related fraud accounted for 55 percent of all fraud reports to the FTC. Losses associated with Internet-related fraud were estimated to approach $200 million.

Two years ago, the Director of the FTC testified before this Subcommittee on the relation between accurate Whois data and the FTC's ability to protect the public. Quote, "It is hard to overstate the importance of accurate Whois data to our Internet investigations. In all of our investigations against Internet companies, one of the first tools FTC investigators use to identify wrongdoers is the Whois database. We cannot easily sue fraudsters if we cannot find them," end quote, and that's a statement of the Honorable J. Howard Beales, III, Director of the FTC.

But Whois data is of little or no use to the FTC or anyone else if registrars who are contractually obligated to verify its accuracy refuse to do so. Similarly, it is also of no use if registrants perceive there to be no credible deterrent or sanction for providing fraudulent data.

The Government must play a greater role in punishing those who conceal their identities online, particularly when they do so in furtherance of a serious Federal criminal offense or in violation of a federally protected intellectual property right. These individuals impose real and substantial cost on legitimate users of the Internet. There is a growing recognition that both registrants who provide false Whois as well as those who enable them to remain anonymous must be held accountable.

The Fraudulent Online Identity Sanctions Act is a targeted measure that will complement related provisions that were recently included in the PROTECT Act and in the CAN-SPAM bill.

This concludes my opening statement. Before recognizing the gentleman from California for his, let me just say at the outset that the testimony that we received today was uniformly superb. It did exactly what I hoped it would do, which was to suggest to the Members of this Subcommittee what changes, what additions, what modifications we can make to the bill to make it a better piece of legislation, and every one of you all have made specific and substantive and practical suggestions for us to modify this bill and I would certainly expect before we get to markup next month that there will be a substantial amendment in the nature of a substitute as a result of the testimony that we expect to receive here today momentarily.

Second of all, I want to thank David Whitney, who is the Subcommittee counsel who put on this, or helped arrange this hearing.

We had to switch this hearing with one that is now scheduled for next week, so on very short notice and with just a few days to pull together this hearing, David Whitney was able to do so in a superb manner. In fact, one night he had to stay up until 3 a.m. to try to work out the kinks to make this run smoothly today. So I appreciate his effort very, very much.

And lastly, we are going to hold our witnesses strictly to the 5 minute limit and try to recognize all the Members for their questions and conclude by 11:00, when a joint session of Congress is scheduled. So that is the reason to kind of expedite this hearing today if at all possible.

Having said all that, I'm now happy to recognize the Ranking Member, Mr. Berman, for his opening statement.

Mr. BERMAN. Thank you very much, Mr. Chairman, and I'll try and speak quickly so we can achieve the goal. I appreciate your holding the hearing. The issue of Internet domain name fraud is not a new one for our Subcommittee, but what I'm happy to say is we're now beginning to embark on an effort to find some legislative solutions.

We've already documented through a series of hearings how inaccurate Whois data hampers law enforcement investigation, facilitates consumer fraud, impairs copyright and trademark protection, imperils computer security, enables identity theft, and weakens private protection efforts.

Although the Commerce Department appears to recognize the problem of inaccurate Whois data, the time has come for Congress to act. In sections 303 and 305 of the legislation, H.R. 2752, the legislation that Mr. Conyers and I introduced, we took one stab at crafting a solution. After taking into account various criticisms, including privacy concerns, Chairman Smith and I decided to try a different approach.

Therefore, we introduce a bill before us today which uses a similar underlying principle, that of penalizing those who submit false or misleading domain name information while addressing the privacy issues raised with Mr. Conyers' and my approach. I believe this legislation will start to rectify the problem of inaccurate Whois data.

It focuses on three initiatives. The first provides for a sentencing enhancement when an individual uses false or misleading data in furtherance of a criminal offense. The other two provisions entail amending the copyright and trademark statutes to allow for an enhanced penalty for a civil violation committed in connection with the provision of false contact information.

These are good initial steps. The legislation is crafted in a way that it targets only the bad actors who register false or fraudulent domain name contact information in furtherance of a violation of law, a preexisting violation of law. Furthermore, this legislation provides for the possibility of increased damages in civil copyright and trademark infringement cases where false or misleading information is used knowingly by the registrant most often in his attempt to avoid detection.

I have some concerns that the bill lacks a specific mandate to the Sentencing Commission to craft appropriate sentencing enhance-

ments and I would hope to strengthen the bill by including such a directive before we go to markup.

In last year's hearing on Whois, the FTC testified that traditional scams such as pyramid schemes and false product claims thrive on the Internet. They explain that it's hard to overstate the importance of accurate Whois data to our Internet investigations. One of the first tools they use to investigate these scams and identify wrongdoers is the Whois database. Inaccurate data severely hampers their law enforcement, consumer protection, and investigative abilities.

Another example of the effects of providing false or misleading information relates to the spam problem. I want to just describe an FTC, a specific FTC problem. The FTC and its enforcement powers in our new anti-spam law performed a sting operation to test compliance with the "remove me" or "unsubscribe" options. From e-mail forwarded to the FTC's database of unsolicited commercial e-mails by participating agencies, they culled more than 200 e-mails that purported to allow recipients to remove their name from the spam list. The agency set up dummy e-mail accounts to test the pledges.

They discovered that most of the addresses to which they sent the request were invalid. Most of the "remove me" requests did not get through. Based on information gathered through this operation, the FTC sent 77 letters warning spammers that deceptive removal claims and unsolicited e-mail are illegal. They sent the letters to addresses listed in the Whois database. Sixteen of the 77 letters, or approximately 21 percent, were returned to the FTC because the addresses in the Whois database were inaccurate.

Faulty Whois data seriously imperils the effectiveness of the legislation we just passed relating to spam. It is for this reason that while I support the legislation, I think we haven't gone far enough. The only complete solution would hold the registrars accountable for accurate—inaccurate—the only complete solution would hold the registrars accountable for inaccurate Whois information. We should craft legislation mandating that registrars comply with their registrar accreditation agreements, which require verification and periodic reverification of the information.

This should not be difficult to do. The registrars are already contractually bound to do so, but neither the Commerce Department nor ICANN seems willing to enforce those contracts. As we move forward with the legislation, I hope we can place just such responsibilities on registrars.

I appreciated the Chairman's comments regarding possible refinements and improvements between now and a markup and I urge my colleagues to support the legislation we've introduced.

Mr. SMITH. Thank you, Mr. Berman.

I just want to say I appreciate the attendance of Mr. Jenkins of Tennessee and Mr. Pence of Indiana. I appreciate your interest in the subject at hand.

Let me now introduce our witnesses. Our first witness is Timothy P. Trainer, who has served as President of the International AntiCounterfeiting Coalition, IACC, since September 1999. With approximately 140 members, the IACC is the largest organization

that deals exclusively with issues that relate to the theft of intellectual property.

As President, Mr. Trainer oversees the day-to-day operations of IACC, including its domestic and international enforcement programs. He has worked extensively with Interpol's IP Crime Action Group as well as on intellectual property initiatives in the Newly Independent States of Eastern Europe.

Mr. Trainer has a law degree from the Cleveland Marshall College of law and an M.A. from the University of Pittsburgh. He completed his undergraduate studies at Kent State University and Keio?—Keio University's International Center in Tokyo.

Our second witness is J. Scott Evans, who is a shareholder in the Charlotte intellectual property law office of Adams Evans, where he specializes in the areas of trademark, copyright, unfair competition, and Internet law. Mr. Evans serves as chair of the International Trademark Association's Internet Committee and he will testify in that capacity today. It is worth noting that he also serves as President of ICANN's Intellectual Property Constituency and that he served as one of the principal authors of ICANN's Uniform Dispute Resolution Policy.

A native Texan, Mr. Evans received his undergraduate degree from Baylor University and his J.D. from the University of Louisville.

Our third witness is Rick Wesson, who is the CEO of Alice's Registry, an ICANN accredited registrar that has developed and marketed their fraud detection system to other registrars in the ICANN community. Mr. Wesson serves as both Vice Chair and Chief Technical Officer of ICANN's Registrars' Constituency and is a member of ICANN's Security and Stability Committee. His testimony today reflects his own views and experiences and is not presented on behalf of either ICANN or other registrars.

Our remaining witness is Mark Bohannon, General Counsel and Senior Vice President of Public Policy for the Software and Information Industry Association, SIIA. In that capacity, Mr. Bohannon is responsible for the legal and public policy agenda of SIIA, including issues that involve privacy, e-commerce, intellectual property protection, and Internet security. His testimony will be presented on behalf of the Copyright Coalition on Domain Names, an organization whose principal goals are to maintain public access to Whois data and to improve its accuracy and reliability.

Another Texan, Mr. Bohannon graduated from the School of Foreign Service at Georgetown University and George Washington University Law School.

Welcome to you all. We have written statements from all the witnesses today and without objection, the complete statements will be made a part of the record.

Mr. Trainer, we will begin with you.

**STATEMENT OF TIMOTHY P. TRAINER, PRESIDENT, INTERNATIONAL ANTICOUNTERFEITING COALITION, INCORPORATED (IACC)**

Mr. TRAINER. Thank you, Mr. Chairman, Mr. Berman, and Members of the Subcommittee. Good morning. On behalf of the IACC, I thank the Committee for the opportunity to testify on the issue

that impacts intellectual property owners, Internet users, and the public at large, the collection, availability, use, and most importantly, the accuracy of identification information collected from domain name registrants by the registrars. We commend the Subcommittee on the proposals that it has put forth for our consideration and we look forward to continuing our cooperative efforts.

The IACC represents a cross-section of industries, including automotive, electric, software, luxury goods, personal care, and pharmaceutical sectors. We are prepared to work with the Subcommittee toward passage of a bill that provides effective protection of intellectual property—to intellectual property owners and will result in a more effective Whois system. We seek provisions that deliver what the registrar accreditation agreement promises and that respond to the Internet users' ability to use Whois effectively.

One thing is clear. Whois is still problematic and is illustrated by the list we have provided which identifies registered names that have inaccurate and/or false contact information. In July 2001, I testified before this Subcommittee stating that the Whois database not only needed to be publicly accessible, but accurate. I also stated that rather than legislation, the registrars needed to meet the obligations of their agreement by ensuring the accuracy of information that is provided. This hearing is evidence that the hoped for improvements of Whois have not occurred.

Today, we address two general issues, first, the ongoing problems of Whois and the resulting elements of the current problems; second, I will address the extent to which the proposed amendment might address the problem.

Essentially, two fundamental shortcomings undermine confidence and reliance on Whois, inadequate obligations on registrars to check information submitted by applicants for registered names and the ease of applicants to submit false information and continue using registered names.

The registrar receives information and is required to obtain and maintain this information and the registered name holders must enter into a registration agreement with registrars and provide a minimum amount of accurate and up-to-date information regarding their contact information. Despite the agreement, deterrence is inadequate to stop the practice of individuals obtaining registered names by using false information.

Applicants have provided bogus telephone numbers, city names, zip codes, and have successfully obtained registered names, indicating an absence of registrar oversight. There are times when existing addresses are used, but not one that actually belongs to the person operating the registered name.

Another ploy of those who trade in counterfeit goods is to use a proxy service to obtain registered names so that the contact information belongs to the proxy service, which in turn may not have received accurate information from the person who seeks anonymity in the first place, adding another layer for the person seeking to be beyond the reach of the authorities, intellectual property owners, and consumers.

Even if the information was initially accurate, members have reported that attempts to contact registered name holders have been

time consuming and expensive because information is not updated. One trademark owner attempting to resolve a trademark infringement case found that a business having a New York City address and contact information had moved to New Jersey 2 years earlier. The information about current location was obtained by the trademark owner's attorney going to the old address, learning that the business had moved, and checking records held by the State, not the registrar's Whois database.

A glance at the list of registered names we have provided leaves no question as to why false names would be used. One member company reported at least 15 cases of false Whois information during the past year when it tried to pursue those offering counterfeit goods. These sites facilitate the trade in counterfeit merchandise. It is difficult to believe that any verification efforts are made.

Regarding the proposed section 1117(e), we recommend that the provision be broad enough to subject persons submitting any false information to these penalties. Essentially, anyone deliberately submitting any false information could be punished by the provisions of this bill. Thus, in addition to the information such as an address, telephone, and facsimile number, this could include Internet protocol addresses and other possible information.

Next, in addition to the violator who provided the false information, we recommend the provision also aim to subject the person who caused this false information to be provided to a registrar. The IACC would support including penalties against persons who register and obtain names that are never used in connection with an online location. This would subject those who obtain registered names that are used for false information but do not have active websites to the penalties intended by this proposal.

In addition, the IACC members believe that the proposal could be broadened to impose liability on parties who, having initially provided accurate information to obtain the registered name, thereafter fail to provide updated information. The current proposal addresses the act of affirmatively providing false information, but not willful refusals or failure to provide valid contact information thereafter.

We also support the criminal sentencing recommendation as reflected in the bill to add the provision to title XVIII, section 3559, although we have no opinion regarding the specific recommendation of 7 years. We hope that the proposal for section 3559 might also include language that appears in the proposed 1117(e), referring to a person acting in concert with a defendant. Similar to our recommendation for 1117(e), we recommend a parallel provision to subject persons causing false information to be provided within the scope of 3559.

I thank the Subcommittee for allowing me to testify and will attempt to answer any questions Members may have. Thank you.

Mr. SMITH. Thank you, Mr. Trainer.

[The prepared statement of Mr. Trainer follows:]

PREPARED STATEMENT OF TIMOTHY P. TRAINER

Mr. Chairman and Members of the SubCommittee, Good morning. I am Timothy Trainer, President of the International AntiCounterfeiting Coalition (IACC). On behalf of the IACC, I would like to thank the Committee for the opportunity to testify on an issue of great importance to intellectual property owners, Internet users, and

the public at large—the collection, availability, use, and, most importantly, the accuracy of identification information collected from domain name registrants by Registrars.

The IACC is the largest organization dealing exclusively with issues involving intellectual property theft. The IACC has approximately 140 members who represent a cross-section of industries, including the automotive, electrical, motion picture, software, sound recording, apparel, luxury goods, personal care and pharmaceutical sectors. The total annual revenues of IACC members exceed US$650 Billion. The objective that brings such diverse industries together is their need to protect their intellectual property and their customers from those who would steal such property.

Initially, we apologize for our short submission on this issue, but will work with the Subcommittee and staff to continue providing input on this issue and this bill. I begin first by underscoring the fact that our comments are limited to the relationship between WHOIS and trademark enforcement issues and the proposed new subparagraph (e) of Section 1117 of Title 15, United States Code and leave to my copyright industry colleague on the panel to address the proposed changes affecting the copyright law and copyright owners. It is clear, however, that most, if not all, trademark owners are also copyright owners and, therefore, we have a significant overlap of interest and agree with the copyright industry's views. Second, on behalf of IACC members, we are prepared to work with the Subcommittee and staff toward passage of a bill that provides effective protection for intellectual property owners and will result in a more effective WHOIS system that assists law abiding parties. We seek provisions that deliver what the Registrar Accreditation Agreement [1] (hereinafter "RAA" or "Agreement") promises and that responds to internet users' ability to use WHOIS effectively.

Although different industries have different experiences and challenges when attempting to protect their intellectual property assets, one thing is clear, WHOIS is still problematic for many companies. In July 2001, I was asked to testify before this Subcommittee and did so, supporting the view that the WHOIS database not only needed to be publicly accessible, but accurate. In addition, I indicated that rather than legislation, the Registrars needed to meet the obligations of the Registrar Accreditation Agreement by ensuring the accuracy of information that is provided by registrants. This hearing is evidence that the hoped-for improvements of WHOIS have not occurred and my members have provided examples of the problems they encounter using WHOIS.

The IACC's testimony will address two general issues. First, I will address the ongoing problems of WHOIS and the resulting elements of the current problems. Second, I will address the extent to which the proposed amendment might address the problem.

## WHOIS: CURRENT PROBLEMS

Essentially, two fundamental shortcomings undermine confidence and reliance on WHOIS:

- Inadequate obligations on Registrars to check information submitted by applicants for Registered Names and
- Ease of applicants to submit false information and continue using registered domain names.

What is commonly referred to as the WHOIS database is the collection of information gathered by a Registrar concerning active Registered Names.[2] On the one hand,

---

[1] Registrar Accreditation Agreement (RAA) (17 May 2001) (Appendices posted: November 25, 2002, January 23, 2003, and April 3, 2003). http://www.icann.org.

[2] RAA at 3.3 *Public Access to Data on Registered Names.* "During the term of this Agreement:

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

3.3.1.1. The name of the Registered Name;

3.3.1.2. The names of the primary nameserver and secondary nameserver(s) for Registered Name;

3.3.1.3 The identity of Registrar (which may be provided through Registrar's website;

3.3.1.4 The original creation date of the registration;

3.3.1.5 The expiration of the registration;

the Registrar is required to obtain and maintain this information. On the other hand, the Registered Name Holders must enter into a registration agreement with Registrars and provide a minimum amount of accurate and up to date information regarding their contact information.[3] Despite the RAA's provisions, there is not sufficient deterrence to stop the practice of individuals obtaining Registered Names by using false information. Some applicants have provided clearly bogus telephone numbers (000–000–0000 or 555–555–5555), cities (Blahville, AH), zip codes (00000) or indicated that the contact information is not available (N/A) and have still successfully obtained Registered Names, indicating an absence of oversight by Registrars. There are times when existing addresses are used, but not one that actually belongs to the person operating the Registered Name. Another ploy of those who trade in counterfeit goods is to use a proxy service to obtain a Registered Name so that the contact information is that of the proxy service, which in turn may not have received accurate information from the person who seeks anonymity in the first place. This adds another layer for the person seeking to remain beyond the reach of the authorities, intellectual property owners, or consumers.

To the extent that the information was initially accurate, members have reported that attempts to contact some Registered Name Holders have been time consuming and expensive because information is not updated. One trademark owner, attempting to resolve a trademark infringement case, found that a business having a New York City address and contact information had moved to New Jersey two years earlier. The information about current location was obtained by the trademark owner's attorney going to the old address, learning that the business had moved and checking records held by the state, not the Registrar's WHOIS database.

Based on our efforts to prepare for this hearing, members have provided a list of Registered Names that all had false information in the WHOIS database. A glance at the list leaves no question as to why false contact information would be used. One member company reported at least 15 cases of false WHOIS information during the past year when it tried to pursue those offering counterfeit goods. These sites facilitate the trade in counterfeit merchandise. As long as a name, phone num-

---

3.3.1.6 The name and postal address of the Registered Name Holder

3.3.1.7 The name, postal address, e-mail address, voice telephone number and (where available) fax number of the technical contact for the Registered Name; and

3.3.1.8 The name, postal address, e-mail address, voice telephone number and (where available) fax number of the administrative contact for the Registered Name.

[3] 3.7.7 Registrar shall require all Registered Name Holders to enter into an electronic or paper registration agreement with Registrar including at least the following provisions:

3.7.7.1 The Registered Name Holder shall provide to Registrar accurate and reliable contact details and promptly correct and update them during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder; name of authorized person for contact purposes in the case of an Registered Name Holder that is an organization, association, or corporation; and the data elements listed in Subsections 3.3.1.2, 3.3.1.7 and 3.3.1.8.

3.7.7.2 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.

3.7.7.3 Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name. A Registered Name Holder licensing use of a Registered Name according to this provision shall accept liability for harm caused by wrongful use of the Registered Name, unless it promptly discloses the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm.

3.7.7.4 Registrar shall provide notice to each new or renewed Registered Name Holder stating:

3.7.7.4.1 The purposes for which any Personal Data collected from the applicant are intended;

3.7.7.4.2 The intended recipients or categories of recipients of the data (including the Registry Operator and others who will receive the data from Registry Operator);

3.7.7.4.3 Which data are obligatory and which data, if any, are voluntary; and

3.7.7.4.4 How the Registered Name Holder or data subject can access and, if necessary, rectify the data held about them.

ber and other contact information appear to be legitimate, there is no verification by the Registrars, despite the language of the Agreement to verify the information.[4]

The list of sites having false contact information associated with them has resulted in increased investigative and legal costs to the trademark owners. It is the IACC's position that the accuracy of registrant information is critical to allowing intellectual property owners to enforce their rights over the Internet and for providing consumers with some recourse against counterfeiters and pirates.

If a businessman wants to acquire a Registered Name, if a parent wants to know who owns the website that is distributing harmful toys, if a consumer wants to know who owns the website that is offering discounted pharmaceuticals, or if a trademark or copyright owner wants to know who owns the Registered Name from which a counterfeit version of its products are being sold, they have one place to turn—WHOIS. We commend this effort to impose higher penalties on persons who deliberately disregard their obligations and submit false information. However, half of the problem may rest with the Registrars because of the absence of an effective method of verifying the information submitted to them, including cases in which the requested name appears suspicious on its face.

Registrars, once on notice of false contact information, should be subject to a requirement that in such a case they must contact the registrant and if no accurate and verifiable contact information is provided in a short, fixed period of time, the site will be shut down. It is clear from the information collected by our members that the Registrars are not fulfilling their obligations to ensure the accuracy of the information it is receiving. Registrars should also have increased obligations to verify the information.

PROPOSED AMENDMENT 15 U.S.C. 1117 AND CRIMINAL PENALTY

The Subcommittee has proposed the following language to be added to Title 15 U.S.C. 1117(e):

> "(e) In a case of a violation under this section, occurring at or in connection with an online location, the violation shall be considered to be willful for purposes of this section if the violator, or a person acting in concert with the violator, knowingly provided material and misleading false contact information to a domain name registrar, domain name registry, or other domain name registration authority in registering a domain name used in connection with the online location, or in maintaining or renewing such registration."

The IACC commends the effort to impose greater liability on those who provide false information regarding their contact information. The deterrent effect of the provision will depend upon the willingness of federal prosecutors to take cases and use these provisions in any prosecution of counterfeiting cases to increase penalties.

Regarding the specific language, there is no current definition for "online location". For specificity, this may mean the Registered Name for the domain name used by the person who has provided false contact information.

Next, we recommend that the provision be broad enough to subject persons submitting any false information to these penalties. Essentially, anyone deliberately submitting any false information could be punished by the provisions of this bill. Thus, in addition to information such as an address, telephone and facsimile number, this could include internet protocol addresses and other possible information.

In addition, in view of the existence of a definition of "violator" as referenced in 15 USC 1114(2)(E), a clarification may be necessary to avoid any confusion.

Next, in addition to the violator who provided the false information, we recommend that the provision also subject a person who causes false information to be provided to a Registrar to be sanctioned. Under the proposed language, it appears to be the intent that both a violator and a person acting in concert can brought within the scope of the provision.

The IACC would support the proposal's applicability to persons who register and obtain names that are never "used in connection with the online location". This would subject those who obtain Registered Names through the use of false information, but do not have active websites, to the penalties intended by this proposal.

---

[4] RAA at 3.7.8 Registrar shall abide by any specifications or policies established according to Section 4 requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of which such information. 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.

In addition, IACC members believe that the proposal could be broadened to impose liability on parties who, having initially provided accurate information to obtain the Registered Name, thereafter fail to provide updated information. The current proposal addresses acts of affirmatively providing false information, but not willful refusals or failure to provide valid contact information thereafter. Registered Name Holders should be required to provide valid contact information not only upon renewal, but also during the course of each registration period within a certain period of time after the former contact information is no longer valid. This is asking Registered Name Holders to do nothing more than individuals are asked to do with a driver's license when there is a change of residential address or one moves to a new state and needs to obtain a new license.

The IACC also supports the criminal sentencing recommendation as reflected in the bill to add the provision to Title 18, U.S.C. Section 3559, although we have no opinion regarding the specific recommendation of seven years.

Regarding the actual text of the proposed new paragraph in Section 3559, the IACC is interested in learning of the possibility of including similar language in this Section that appears in the proposed 15 U.S.C. 1117(e), referring to a person acting in concert with the defendant. Similar to our recommendation for 1117(e), we recommend a parallel provision to subject persons causing false information to be provided to be within the scope of Section 3559. This would encompass offenders who either directly submit false information or cause false information to be submitted.

> "(e) SENTENCING ENHANCEMENT FOR FALSIFICATION RELATING TO DOMAIN NAMES IN CONNECTION WITH OFFENSES.—The maximum imprisonment otherwise provided by law for a felony offense shall be increased by 7 years if, in furtherance of that offense, the defendant knowingly provided material and misleading false contact information to a domain name registrar, domain name registry, or other domain name registration authority in connection with a domain name registration. For purposes of this subsection, the term 'domain name' has the meaning given that term in section 45 of the Act entitled 'An Act to provide for the registration and protection of trademarks used in commerce, to carry out the provisions of certain international conventions, and for other purposes' approved July 5, 1946 (commonly referred to as the 'Trademark Act of 1946'; 15 U.S.C. 1127)."

Given the linkage of this provision to another felony offense, it would seem that a defendant would have to be found guilty of trafficking in counterfeit goods under 18 U.S.C. 2320 to have this as a possible sentencing departure for the add-on. We would hope that this might encourage more federal prosecutors to accept counterfeiting cases.

## CONCLUSION

The IACC appreciates the opportunity to testify before the Subcommittee and will be happy to work with the Subcommittee in moving this bill forward. The IACC and its members will endeavor to provide information when possible. I will attempt to answer any questions the Members may have.

ATTACHMENT

**Web sites with False WHOIS Information**

2004watch.com
Allreplicas.com
Authenticstyles.com
Barbiehandbags.com
Basement-prices.com
Clubreplica.com
Deluxwatches.com
DSforless.com
Elitereplicawatches.com
Eurofakes.com
Eurotimesinc.com
Everyswiss.com
Exclusivereplicas.com
Fakeoakleys.com
Fancyfakes.com
Finereplicawatch.com
Fineluxurytime.com.cn
Fineluxurytime.net
Finewatchreplicas.com
Foxyfash.com
Getthatlook.com
Globalreplicas.com
Go-replicas.com
Goreplicas.com
Gradeoneswiss.com
Howtobeaplaya.com
Idealwatches.com
Identicalwatches.com
Ilovemyreplica.com
Knockoffbagsnmore.com
Luxuryreplicas.com
Megawatchsale.com
Myreplicaswatch.com
Paradisewholesale.com
Perfectswiss.com
Planetreplica.com
Preciseknockoffs.com
Qualityhanbags.com
Replica-planet.com
Replicabiz.com
Replicacenter.com
Replicadetails.com
Replicagenuine.com
Replicagod.com
Replicaking.com
Replicalord.com
Replicanews.com
Replicaoakley.net
Replicapalace.com
Replicasonstock.com
Replicasworld.com
Replicawatch.us
Replicawatches.com
Solidreplicas.com
Swiss-copies.com
Swisswatchreplica.com
Time4replicas.com
Unlimitedreplicas.com
Urbanmusic2000.com
Watchesperfection.com
Watchreplica1.com
Warehousetimes.com

**Examples of Contact Information**

24hrcigarette.com
n/a n/a
Fax: n/a
n/a
n/a, NJ n/a
USA

Moresmoke.com
Stern Enterprises
1212 Blah Ave
Blahville, AH 11112

Mr. SMITH. Mr. Evans.

**STATEMENT OF J. SCOTT EVANS, CHAIRMAN, INTERNET COMMITTEE, INTERNATIONAL TRADEMARK ASSOCIATION (INTA)**

Mr. EVANS. Good morning, Mr. Chairman. The International Trademark Association appreciates very much your invitation to testify on ways in which we can improve the accuracy of Whois, the database that contains contact information on registered domain names.

INTA, which has served as the voice of trademark owners during the ongoing international debate on the running of the domain name system, is grateful to this Subcommittee for its diligence in ensuring that trademark owners have the right tools to protect their intellectual property in cyberspace and that consumers can make safe and informed choices when working online.

This Subcommittee has already provided tremendous assistance by highlighting the importance of Whois, and through hearings like the one held last September, as well as through frequent contacts with the Department of Commerce and the Internet Corporation for Assigned Names and Numbers, also known as ICANN. Subcommittee Members know how important accurate Whois data is for intellectual property owners, law enforcement, and consumer protection interests.

Only with access to accurate and up-to-date Whois data can the Internet be a safe environment that people and businesses can rely on with confidence. Only with accurate Whois data can trademark owners more easily resolve cybersquatting disputes and learn the contact details for owners of websites offering counterfeit products.

ICANN has in place a registrar accreditation agreement that requires each domain name registrant to provide to domain name registrars accurate and reliable contact details. Domain name registrants are further required to promptly correct and update those details during the term of the registration. Unfortunately, despite these requirements, trademark owners have for many years been encountering instances of blatantly inaccurate or missing data, often from fictitious entities listing false addresses, as well as information that is simply out of date.

My written statement lists several examples where trademark owners like Kodak, Nintendo, Nokia, and even the USO have encountered patently inaccurate Whois data when attempting to track down cybersquatters and online counterfeiters. This is not even the tip of the iceberg.

There are thousands of examples where a trademark owner finds that the registrant of a domain name that is infringing its rights lives on Darth Avenue in Vader, California, or on Small Wok Way in Chopsticks Town, Wisconsin. Some of the more interesting names used by cybersquatters and counterfeiters are Buy This Name, or Nuclear Marshmallows, and even millionaire Thurston Howell III, who along with Gilligan resided on that uncharted desert isle we all tuned in to watch during the 1960's.

Some people might find this amusing, and if there wasn't so much at stake in terms of time and expense for trademark owners and safety and reliability for consumers, we might be able to laugh, as well. But there is a lot to be worried about. The problem of inac-

curate Whois data and the failure on the part of domain name registrars and ICANN to enforce the provisions of the RAA has reached the point where many trademark owners no longer rely on Whois. It is simply too expensive and too time consuming and there is little prospect of positive results. Instead, trademark owners are forced to hire private investigators, sometimes at great expense, and, of course, consumers don't even have that option.

There have been some recent attempts by ICANN to begin to address the problems of inaccurate Whois data. For example, thanks in large part to the efforts of this Subcommittee, amendment 6 to ICANN's and the Commerce Department's MOU includes a requirement that ICANN continue to assess the operation of Whois, implement measures to secure improved accuracy, and develop a strategic plan that includes a system for auditing material contracts like the RAA for compliance by all parties to such agreements. Once again, however, despite what appears in black and white, as well as repeated pleas by the intellectual property community, we have not seen any concrete steps by ICANN or domain name registrars to improve Whois accuracy.

INTA, therefore, supports your efforts, Mr. Chairman, as well as those of Ranking Member Berman, to try and develop new statutory tools that will help accomplish this goal. We have recently received the Fraudulent Online Identity Sanctions Act from the Subcommittee staff and are in the process of reviewing the proposed language, which would amend the damages section of the Lanham Act. INTA looks forward to working closely with the Subcommittee and its staff to develop statutory language that will command the most support and strengthen the safety of online commerce by helping to ensure that domain name registrants provide accurate and reliable data for the Whois database.

This concludes my opening statement. I thank the Subcommittee once again for the invitation to testify. I would be pleased to answer your questions.

Mr. SMITH. Thank you, Mr. Evans.

[The prepared statement of Mr. Evans follows:]

PREPARED STATEMENT OF J. SCOTT EVANS

I. INTRODUCTION

Good morning, Mr. Chairman. My name is J. Scott Evans. I currently serve as chairman of the Internet Committee of the International Trademark Association (INTA). I am a shareholder in the firm of Adams Evans, which is an INTA member. As do all INTA officers, board members and committee members, I serve on a voluntary basis. In addition to my volunteer service with INTA, I also volunteer as president of the Intellectual Property Constituency of the Internet Corporation for Assigned Names and Numbers (ICANN).[1] My appearance before the subcommittee, however, is only on behalf of INTA.

INTA is pleased to be here today to offer testimony in connection with this subcommittee's efforts to develop new criminal and civil enforcement tools to help curb online fraud.

[1] "The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function." *http://www.icann.org/general/*.

## II. ABOUT INTA

INTA is a 126-year-old not-for-profit organization comprised of over 4,300 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 domain name system (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.

## III. THE WHOIS DATABASE

### *A. Whois and Uses By Trademark Owners*

INTA is grateful to this subcommittee for its diligence in ensuring that trademark owners have the proper safeguards in order to protect their intellectual property in cyberspace. Measures such as the "Anticybersquatting Consumer Protection Act,"[2] have helped tremendously in curbing online bad-faith activity that harms not only trademark owners, but, more importantly, consumers who rely on trademarks to provide information that will enable them to make important decisions about the goods and services they purchase.

Also, we are very pleased with your leadership, Mr. Chairman, in taking such a strong interest in the critical issue of ensuring the accuracy of contact data on registered domain names, which is typically known as "Whois."[3] Whois serves a vital role in preventing domain name fraud. Its uses include: law enforcement, consumer protection, and the protection of intellectual property rights. Only with access to accurate and up-to-date Whois data can the Internet be a safe environment that consumers can rely on with confidence. Trademark owners value Whois data in order to resolve domain name disputes (e.g., cybersquatting), 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.

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 domain name registrar's website, finding the icon labeled "Whois," "clicking," and typing in a particular domain name; and (2) bulk Whois data that is the whole of a particular registrar's database, which can be purchased from a registrar. Trademark owners use both types of Whois.

### *B. ICANN Whois Requirements*

Since November 1998, the United States Government (USG) through a memorandum of understanding (MOU) has entrusted administration of the DNS to ICANN. Amendment 6 to the MOU was entered into on September 17, 2003, extending the relationship between the USG and ICANN for another three years.[4]

ICANN, upon its formation and as part of its initiative to expand the number of domain name registrars,[5] crafted the Registrar Accreditation Agreement (RAA), 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.[6] This includes the familiar suffixes of .com, .net, and .org, as well as gTLDs that were approved by ICANN in 2000: .info, .biz, .name, .pro, .museum, .coop, and .aero. In particular, the RAA requires that ICANN accredited registrars 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.[7]

---

[2] Pub. L. No. 106–113, § 3002, 113 Stat. 1501, 1537 (1999) (amending 15 U.S.C. § 1125).

[3] *See, e.g.,* Letter from Chairman Smith and Ranking Member Berman to Secretary of Commerce Donald Evans regarding developments that affect the operation of the Internet, August 8, 2003 ("[I]t is vitally important to ensure public access to online systems like Whois."); Oversight Hearing on *Internet Domain Name Fraud—the U.S. Government's Role in Ensuring Public Access to Accurate Whois Data,* September 4, 2003.

[4] *See http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6—09162003.htm.*

[5] Today there are approximately 167 ICANN accredited registrars from 25 countries. *http://www.icann.org/registrars/accredited-list.html.*

[6] RAA, at *http://www.icann.org/registrars/ra-agreement-17may01.htm.*

[7] *Id.* at para. 3.7.7.1.

*C. Problems with Whois Accuracy*

Unfortunately, despite the RAA requirement that registrants provide "accurate and reliable contact details," trademark owners have for many years been encountering instances of blatantly 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 Uniform Dispute Resolution Policy (UDRP)[8] case involving the cybersquatting of *www.nhlpenguins.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." The contact address listed in the Whois records was the Russian Institute of Physics and Power Engineering in a town 100 kilometers south of Moscow.[9]

(2) When attempting to track down the registrant of *www.wwwsportauthority.com,* the Sports Authority found that the name of the registrant was replaced with a pornographic phrase.

(3) The domain name *www.kodakphotospot.com,* was listed by its owner as being for sale, does not provide an owner, administrative, or technical contact address.

(4) Intel Corporation discovered that a cybersquatter registered the domain name *www.intel64fund.com.* (The Intel 64 Fund is a quarter billion dollar equity investment fund that invests in certain technology companies.) The domain name linked to a pornographic site. The Whois information provided by the registrar listed "Buy This Name" as the owner. Also, in a dispute involving *www.pentium.org,* Intel found that the registrant's address listed in the Whois database was a P.O. Box without a P.O. Box number.

(5) In attempting to track down the owner of *www.Nokia-uk.com,* Nokia, the mobile communications company, found that the domain name was registered in the name of: "European Distributor, Nokia UK Limited, Nokia Venture Partner, GB-Farnborough, GU14 0NG." The domain name was used to send emails falsely representing that the sender was from Nokia. Anyone checking the Whois directory would have believed the owner of the domain name to be Nokia UK Ltd., which is based in Farnborough, UK.

(6) For the domain name *www.harleydavidsonmotorcompany.net,* counsel investigating the ownership of the name found the telephone and fax numbers were listed as "+1.11111111111" in the Whois database.

(7) Internet services company Verio discovered that the registrant for the domain name *www.1verio.com* was "sunshinehh." The listed email address, which was *f@hotmail.com,* was not operative, and attempts to send email to it resulted in a bounce back.[10]

(8) 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."

(9) When Nintendo attempted to track down the registrant of a domain name that corresponded to one of its popular Pokémon characters, *www.gyrados.org,* it found that contact fields in Whois were filled with nonsense, such as "asdasdsdaasdsa."

(10) In an attempt to track down the owner of a website that was selling unauthorized "USO Care Packages" online, the United Service Organizations (USO) found that the Whois information listed an address in the Faeroe Islands (between Iceland and Norway, administered by Denmark). This address was not real. The USO has thus far been unable to locate the registrant. As a result, there remains potential consumer confusion and poten-

---

[8] "All ICANN-accredited registrars follow a uniform dispute resolution policy. . . . In disputes arising from registrations allegedly made abusively (such as 'cybersquatting' and 'cyberpiracy'), the uniform policy provides an expedited administrative procedure to allow the dispute to be resolved without the cost and delays often encountered in court litigation." *http://www.icann.org/general/glossary.htm#U.*

[9] *National Hockey League And Lemieux Group Lp* v. *Domain For Sale,* IPO Mediation and Arbitration Center, Administrative Panel Decision Case No. D2001–1185.

[10] *http://arbiter.wipo.int/domains/decisions/html/2003/d2003–0255.html.*

> tial loss of goodwill for the USO if the "care packages" contain goods of inferior quality.[11]

Other examples of bad Whois data have included addresses like "Small Wok Way, Chopsticks Town, WI 00000" and "1412 Darth Ave., Vader, CA 93702," and domain name registrants listed as "Nuclear Marshmallows" and "Thurston Howell III," a character from the television show "Gilligan's Island."[12] One might consider these blatantly false Whois entries as amusing.[13] But, the truth is, they cost brand owners a great deal in terms of time and expense, and they put consumers at great risk.

Supposedly, 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 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.

Regardless of these provisions, many accredited registrars have been lax in investigating and cleaning up registrations with false Whois data. The problem of inaccurate Whois data and the failure on the part of domain name registrars to ensure reliable data has reached the point that many trademark owners no longer seek assistance from the domain name registrar. It is simply too time consuming and there is little prospect of positive results. Instead, trademark owners are forced to hire private investigators, sometimes at considerable expense, 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.[14] 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.[15] 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.

*D. DOC/ICANN MOU Amendments*

There have been some recent attempts by ICANN to begin to address the problem of inaccurate Whois data. For example, thanks in large part to the efforts of this subcommittee, Amendment 6 to the MOU, which I referenced earlier, includes a requirement that ICANN, "Continue to assess the operation of WHOIS databases and

---

[11] *See http://www.all-worlds-shopping.com/gifts&flowers/care%20packages/uso-care-packages.htm.* Whois information at *http://www.betterwhois.com/bwhois.cgi?domain=all-worlds-shopping.com&x=42&y=15.*

[12] *U.S. Franchise System* v. *Thurston Howell III,* National Arbitration Forum, Claim Number: FA0303000152457, at *http://www.arb-forum.com/domains/decisions/152457.htm.*

[13] "The Professor's scientific prowess is not in dispute in this case, yet the Panel doubts that he would be able to create a means of accessing the Internet from little more than coconuts and knowledge of the type of technology that existed decades ago. Respondent can obviously afford to register a domain name; what is doubtful is the means (or desire) to do so from an uncharted desert isle." *Id.* at fn. 1.

[14] In addition to the problems associated with accuracy, it should also be noted that trademark owners continue to have problems with respect to registrars granting accessibility to bulk Whois data. See, e.g. Letter from Jane Mutimear, then-president of the ICANN IPC to ICANN's then-general counsel Louis Touton, May 1, 2003, at *http://www.icann.org/correspondence/mutimear-to-touton-01may03.htm* ("Denial of such access is a violation of the RAA, something that falls squarely within the purview of ICANN's enforcement responsibilities."). We understand, however, that accessibility is not the focus of this hearing, but nonetheless want to state that accessibility remains of equal concern to INTA members.

[15] 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.*

to implement measures to secure improved accuracy of WHOIS data,"[16] as well as, by December 31, 2003, develop a strategic plan that includes a review and augmentation of ICANN's corporate compliance program, "including its system for auditing material contracts for compliance by all parties to such agreements."[17]

IV. LEGISLATIVE OPTIONS

Once again, despite what appears in "black and white" in the MOU and the RAA, as well as repeated pleas by the intellectual property community, we have not seen any concrete steps by ICANN or domain name registrars to improve Whois accuracy. INTA therefore, supports your efforts, Mr. Chairman, as well as those of Ranking Member Berman, to try and develop new statutory tools that will help accomplish this goal. The subcommittee staff has recently shared with INTA the "Fraudulent Online Identity Sanctions Act," which would add a new Section 35(e) to the Lanham Act to make a violation specified in that section (*i.e.,* infringement, dilution, counterfeiting, and cybersquatting) "willful" if it is committed in connection with an online site and with the provision of false registrant contact data. Proof of willfulness would permit a judge to impose higher monetary penalties against a defendant.

While INTA is currently in the process of reviewing the proposed approach and language in the "Fraudulent Online Identity Sanctions Act," particularly with regard to the broader implications for trademark law generally of expressly identifying one type of willful misconduct in the statute,[18] we believe that the subcommittee is moving in the right direction in pursuing the concept of greater penalties against those who provide false Whois data. INTA, therefore, would very much like to work closely with this subcommittee and its staff to develop statutory language that will command the most support.

V. CONCLUSION

Thank you for the opportunity to testify. Where accurate Whois information has been provided, trademark owners can often amicably resolve problems quickly and without the need to resort to legal proceedings, and the interests of consumers are well served. INTA looks forward to working with this subcommittee to strengthen the safety and reliability of the DNS and, in particular, to improve the accuracy of Whois data.

Mr. SMITH. Mr. Wesson.

## STATEMENT OF RICK H. WESSON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ALICE'S REGISTRY, INCORPORATED

Mr. WESSON. Thank you very much, Chairman Smith, Ranking Member Berman, and Members of the Subcommittee for this opportunity to testify on this important subject.

I have followed and participated in Whois issues for nearly a decade. When a member of Mr. Berman's staff came to discuss intellectual property issues with the Registrars' Constituency at one of our interim meetings in Washington, D.C., the staffer enumerated the issues of Whois accuracy. He spoke of such problems as invalid and missing registrant data and provided examples that were obviously incorrect to even the most basic validation would have identified the domains as lacking correct or valid information.

I initially thought that this task was too complicated and impossible and set out to prove myself wrong. Beginning in 2001, I spent

[16] This includes a requirement that ICANN "publish a report no later than March 31, 2004, and annually thereafter, providing statistical and narrative information on community experiences with the Whois Data Problems Reports system." To date, INTA has not seen any increased effort by ICANN to publicize this system in order to collect data.

[17] MOU, Amendment 6, Article II (C)(10) & 14(d), at *http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6—09162003.htm*

[18] The question of what is a "willful" act under trademark law remains a subject of debate. *See, e.g.,* Koelemay, "A Practical Guide to Monetary Relief in Trademark Infringement Cases," 85 Trademark Rep. 263, 270 (1995) ("Those courts that retain a scienter requirement have not defined 'bad-faith' or 'willfulness' consistently. These cases have ranged from holding mere knowledge of the plaintiff's mark sufficient, to requiring a deliberate intention to infringe and to trade on the plaintiff's goodwill.") (Citations omitted).

the next 18 months developing the technology to perform fraud analysis on electronic commerce transactions with the intent of solving the registrars' Whois data accuracy problems. The technology we developed was specifically targeted to identify invalid and undeliverable postal addresses, undeliverable e-mail addresses, and non-dialable telephone numbers.

Understand that customers for Internet domains are a global population and registrars in France sell to customers in the United States and U.S.-based registrars sell domains to registrants in many countries. Performing analysis on the registrant data when the registrant is located in one of over 200 countries is difficult, but not beyond the reach of all Internet-based businesses.

Eventually, we learned how to correlate postal addresses, e-mail addresses, and telephone numbers with IP addresses and verify that they all existed in over 200 countries. Using this technology, we were able to make our business unattractive to individuals looking to fraudulently register domain names. It's simply an artifact of our anti-fraud technology that it prevents invalid registrant data.

A case in point where I encountered fraudulent data occurred last year when some of my computers had been infected with a virus that gave control of the system to a third party without my knowledge. When I tracked down the hacker and discussed with them how I became infected, I learned that the hackers controlled over 3,500 computers, and for a fee, one of the operators offered to perform denial of service attacks on any network that I requested.

I attempted to have the Whois of this domain that they used to perform these attacks deleted. I submitted a Whois update request through ICANN and eventually the domain's incorrect Whois was updated, but the domain was not deleted, allowing distributed denial of service attacks to continue. Shortly after the domain's Whois was updated, it was updated again with bogus information.

Currently, this entire deception is completely legal. The same dynamic directly and immediately impacts trademark and copyright issues exactly the same way.

We launched the service Fraudit, as in Fraud Audit, for registrars to increase their data accuracy at the ICANN—at the 2002 ICANN meeting in Shanghai, China. To our surprise, registrars were somewhat angered to learn that someone had come up with a solution to the Whois data accuracy problem. Registrars appeared to believe that as long as no solution existed, there was no good reason to audit their registrant data. In fact, the only time that they performed self-audits was when the registrar was faced with a financial loss. Registrars have been hit hard with credit card fraud, and one large registrar had a rather embarrassing incident by nearly losing their merchant account, removing their ability to take credit cards over the Internet, all because of fraud.

Although all registrars experience some credit card fraud and most have invested in mitigating that risk, they have not attempted nor invested in the ability to prevent the introduction of fraudulent registrant data. As long as a domain is paid for and the registrar is not hit with a credit card charge-back, there is no business reason to prevent invalid registrant data from the Whois system.

My ultimate realization that ICANN, gTLD registries, and accredited registrars had no intention, desire, or incentive to audit their registrant data caused us to withdraw the product from the Whois accuracy space.

I do support the proposed legislation as a step forward and hope it will deter those intent on registering domains with fraudulent contact data. While it might indeed have a deterrent effect, we cannot solely rely on industry regulation to prevent false and invalid registrant data from entering the Whois database.

As it stands, the proposed legislation does not impact registrars. With no provision barring registrars from accepting fraudulent registrant data or requiring a registrar to prevent registrant—to verify registrant data, I expect the industry to continue on its present course. With no real-time analysis of registrant data on the front end, we're leaving it up to law enforcement to determine the accuracy only during an infringement investigation. With simple regulation, the registrars could validate the accuracy of their Whois data and law enforcement may uphold the law. Without it, law enforcement will just be swimming around in invalid data.

It's that simple. The technology exists, but legislation needs to require a reasonable effort upon registrars' part to use it. Please add a requirement that registrars be involved in validating a potentially accurate representation of those they register. Don't miss this opportunity to evolve the Internet beyond the wild, wild West and to the safety of a civilized community.

Thank you. I'd be happy to answer any questions you have.

Mr. SMITH. Thank you, Mr. Wesson.

[The prepared statement of Mr. Wesson follows:]

PREPARED STATEMENT OF RICK H. WESSON

Thank you very much, Chairman Smith, and Ranking Member Berman, and Members of the Subcommittee for the opportunity to testify on this important subject. In the interests of full disclosure I am the Vice-Chair and Chief Technical Officer of the Registrars Constituency within ICANN and also serve on the ICANN Security and Stability committee. Today I am testifying for my self as President and CEO of Alice's Registry Inc., an ICANN accredited Registrar.

This testimony will address two main issues. First, I will address Whois data accuracy as a function of fraud in domain registrations by ICANN accredited registrars. Second, I will address the issues of this legislation and further goals to peruse.

I've followed and participated in Whois issues for nearly a decade. When a member of Mr. Berman's staff came to discuss IPR issues with the Registrars' Constituency at one of our Interim meetings in Washington, DC, the staffers enumerated the issues of Whois accuracy, such as invalid or missing registrant data, examples given were obviously incorrect and even the most basic validation would have identified the domains as lacking correct or valid information.

Beginning in 2000, I spent the next 18 months developing a technology to perform fraud analysis on electronic commerce transactions with the intent of solving registrars' Whois data accuracy problems. The technology we developed was specifically targeted to identify invalid and undeliverable postal address, undeliverable e-mail address, and nondialable telephone numbers.

Understand that the registrants for Internet domain names are a global population. Registrars in France sell to registrants in the US and US based registrars sell domains to registrants in India and many other countries. Performing analysis on the registrant data when the registrant is located in one of over 200 countries is difficult but not beyond the reach of all but the largest Internet based businesses. We developed Fraudit, our fraud detection technology, because registrants were committing credit card fraud from Eastern Europe using addresses located in 2nt and 3rd world countries.

Typical scams included using cities that did not exist within the country they stated they were in, or telephone numbers that were valid, but proved to be a directory assistance number. Often fraudsters would use e-mail addresses that were undeliverable, telephone numbers that did not exist at all, and postal addresses that could not exist.

Eventually we learned how to correlate the postal address, email address, and telephone numbers with IP addresses and verify that they all exist, in over 200 countries. Using this technology we were able to make our business unattractive to individuals looking to fraudulently register domain names. It is simply an artifact that our anti-fraud technology prevents invalid registrant data.

While it is easy for the untrained eye to see that the domains enumerated in Mr. Trainer's testimony are registered with inaccurate data, we provide three examples of domain name registrations in our written testimony that are more difficult to determine the accuracy of. While the Canadian and US registrations do contain a mix of accurate and inaccurate data, the domain registered to a registrant in INDIA, which appears suspect, is actually correct. Without special knowledge of each countries telephone-numbering plan, postal addressing system and special knowledge of Internet addressing and email delivery no human could be expected to be capable of validating registrant data for over 200 countries.

A case in point where I encountered fraudulent data occurred last year when some of my computers had been infected with a virus that gave control of the system to a third party without my knowledge. When I tracked down the hacker and discussed with them how I became infected I learned the hackers controlled over 3,500 computers and for a fee, one of the operators offered to perform a denial of service attacks on *any network* I requested.

I attempted to have the Whois of the domain that they used to perform these attacks deleted. The domain was igger.com and the host they used to coordinate these attacks from was named n.igger.com. I submitted a Whois update request through ICANN and eventually the domain's incorrect Whois was updated but not deleted, allowing the distributed denial of service attacks to continue. Shortly after the domain's Whois was updated, it was updated again with bogus information. Currently this entire deception is completely legal. The same dynamic directly and immediately impacts trademark and copyright issues exactly the same way.

We launched the service Fraudit, as in "Fraud-Audit", for registrars to increase their data accuracy at the 2002 ICANN meeting in Shanghai, China. To our surprise registrars were somewhat angered to learn that someone had come up with a solution to the Whois data accuracy problem.

Registrars appeared to believe that as long as no solution existed, there was no good reason audit their registrant data. In fact the only time they preformed self-audits is when the registrar was faced with a financial loss. Registrars have been hit hard with credit card fraud. One large registrar had a rather embarrassing incident by nearly loosing their merchant account, removing their ability to take credit cards over the Internet, because of fraud. Although all registrars experience some credit card fraud and most have invested in mitigating that risk, they have not attempted, nor invested in, an ability to prevent the introduction of fraudulent registrant data—as long as the domain is paid for and the registrar is not hit with a credit card charge back there is no business reason to prevent invalid registrant data in the Whois system. My ultimate realization that ICANN, gTLD registries and accredited registrars had no intention, desire, or incentive to audit their registrant data caused us to withdraw the product from the registrar Whois accuracy space.

I do support the proposed legislation as a step forward and hope it will deter those intent on registering domains with fraudulent contact data. While it might indeed have a deterrent effect, we cannot solely rely on industry regulation to prevent false and invalid registrant data from entering the Whois database. As it stands, the proposed legislation does not impact registrars. With no provision barring registrars from accepting fraudulent registrant data or requiring a registrar verify registrant data, I expect the industry to continue on its present course. With no real-time analysis of registrant data on the front end we are leaving it up to law enforcement to determine the accuracy only during an infringement investigation.

With simple regulation that registrars validate the accuracy of their Whois data, then law-enforcement can uphold the law. With out it, law-enforcement will just be swimming around in invalid data. It's that simple. The technology exists, but legislation needs to require a reasonable effort on registrars' part to use it. Please add a requirement that registrars be involved in validating a potentially accurate representation of those they register. Don't miss this opportunity to evolve the Internet beyond the wild, wild west toward the safety of any civilized community.

Again, thank you for this opportunity to testify today and I am happy to answer any questions you have.

# Appendix A

# Example Fraudit Analysis Report

Included below are three example reports of Fraudit analysis of domain names. The first domain appears valid, as all the normal address elements exist in the Whois record. Initial inspection reveals that the phone number is not valid, though almost all of the elements of the record are in fact invalid. The second domain resides in INDIA and appears strange and probably incorrect, though after analysis the domains address information is fairly accurate and has a high probably of being able to contact the registrant via postal mail, e-mail and phone. Finally the last domain appears fairly correct though the postal address is undeliverable as there is no PO box in the indicated zip code.

## Example #1

```
Domain: 123bankruptcy.com

 Registrant
   FDS Digital
   fdsdigitalwhj@hotmail.com
   5525 West Bl 114
   Vancouver, BC 63611 CA
   +1.1111111111
```

- Email address is free-mail site.
- Undeliverable email address, email will bounce.
- Phone is invalid, does not exist in North American dial plan
- Street does not exists in Vancouver, Canada
- Postal code invalid format for Canada

## Example #2

```
Domain Name..... 123wine.com
  Creation Date..... 2001-04-15
  Registration Date.... 2001-04-15
  Expiry Date..... 2004-04-15
Admin Name..... Sohail Roshni
  Admin Address..... "42 olympus, mmc road"
  Admin Address..... mahim west
  Admin Address..... mumbai
  Admin Address..... 400016
  Admin Address..... maharashtra
  Admin Address..... INDIA
  Admin Email..... admin@findjunction.com
  Admin Phone..... 091982135659
  Admin Fax.....
```

Phone is mobile, confirmed.
Postal code for MAHARASHTRA, MAHIM HO INDIA confirmed.
Email address is deliverable, address confirmed.

City Mumbai is City Bombay -- Lat: 18 56 00 N  Long: 072 51 00 E

## Example #3

```
Domain Name: CALIFORNIALOTERY.COM

Administrative Contact:
 Admin, Site admin@acmemail.com
 Box 455
 Miami, FL 33265
 US
 305-210-6453
```

- Phone is USA POTS phone, validated.
- Phone is located in Miami, FL
- Email address is deliverable, address confirmed.
- Postal address is PO Box.
- PO BOX number does not exist in US Zip-Code 33265

FRAUDIT

# Protect yourself from domain name fraud before it starts.

Introducing Fraudit, the first Whois inaccuracy detection technology.

Domain name fraud has been getting a lot of attention recently. And for good reason: research indicates that a significant number of domain name registrations use false information. That number is on the rise as "cybersquatters" find that they can successfully defraud innocent registrants, and federal agencies have a difficult—if not impossible—task in finding and punishing the anonymous perpetrators. For the victims, the damage to their business in terms of time and costs can be irreparable. In the bigger picture, fraud affects the viability of the Internet as a whole, as consumers begin identifying the Internet with fraud.

The solution lies in ensuring the accuracy of Whois data.

Stopping domain name fraud means getting to the heart of the problem: ensuring the accuracy of Whois data. As J. Howard Beales, III, Director of the Federal Trade Commission's Bureau of Consumer Protection, told the House Judiciary Committee's Subcomittee on Courts, the Internet, and Intellectual Property, "It is hard to overstate the importance of accurate Whois data to our Internet investigations. In all of our investigations against Internet companies, one of the first tools FTC investigators use to identify wrongdoers is the Whois database."

Introducing Fraudit—your tool for ensuring accurate Whois data.

Through a simple Web-based form or secure Web-Service, Fraudit allows anyone to verify an entity's email address, postal address and telephone number before embarking on a business venture with them. Fraudit scores the accuracy of registration information, so you can be confident that the company you're dealing with is, or is not, legitimate. Fraudit also gives ICANN and Law Enforcement agencies a good place to start finding and prosecuting online criminals. Fraudit is easy to use, cost-effective, offers a fast response, and is quick to set up and implement. And Fraudit comes from Alice's Registry, the leading supplier of domain name technology.

Detect and deter fraud before it starts: with Fraudit.
Take Fraudit for a FREE test spin.

**Try Fraudit out for yourself. Visit Alice's Registry at www.ar.com for a free demo now!**

**Fraudit stops fraud before it starts through:**

- **Early fraud detection,** which increases revenue: Saves your company costly charge-back fees associated with fraud
- **Front-end automation:** Detects errors on the front end, before fraud hits your bottom line
- **Increased compliance:** Reduce your risk of breaking the law (which you may be doing without even knowing it)
- **Easy implementation:** Client toolkits are written in Perl5 and Java, so you can started quickly with only minor modifications to your signup process
- **Web-friendly user interface:** Registration verification is simplified through color-coded ranked registration data
- **Speed and accuracy:** Fraudit returns an accurate response to your query within seconds.

Mr. SMITH. Mr. Bohannon.

**STATEMENT OF MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, PUBLIC POLICY, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION (SIIA), ON BEHALF OF COPYRIGHT COALITION ON DOMAIN NAMES (CCDN)**

Mr. BOHANNON. Chairman Smith, Representative Berman, Members of the Subcommittee, it's always a privilege and a pleasure to appear before you and I want to commend and thank you for your continued focus on this critical issue to us.

Your hearing last September in particular not only reinforced the critical role of Whois in protecting intellectual property and other vital issues, but it made a very real difference as the Department of Commerce renewed its MOU with ICANN, and I want to put that on the record and make sure that we're clear, that without your help, I don't think we would have gotten what we did in the MOU.

I'm here today on behalf of the Copyright Coalition on Domain Names, which has worked since 1999 on this issue. Our members, who I'm sure you are very familiar with, are listed on the front of our testimony, but represent leaders in software, motion picture, recording, performance rights, and digital content.

I know that and hope that my full testimony will be submitted for the record. Let me just emphasize a couple of points as we go into the question and answer period.

The first is that Whois data is essential and there's not really much I can add to the testimony of my colleagues, the comprehensive record of this Committee, the excellent testimony of Mr. Edelman last September, who documented the fact that many of the domain name registrations for which there is inaccurate Whois data are, in fact, those engaging in illegal infringement and other activities.

The second question is how will your legislation help solve this problem? The Whois database simply cannot perform those critical functions that we've all identified if the data is inaccurate, out of date, or otherwise unreliable. Unfortunately, I doubt there's anyone who has ever stood up and said that the Whois database is something that we can actually rely on.

It's our view that it is time for Congress to act on this problem, and we believe that the legislation on the table at this hearing, H.R. 3754, takes the right approach. The legislation is focused and it is narrowly tailored. It deals solely with those already convicted of serious crimes or found liable for online infringements and who also have tried to hide their tracks, complicate the work of law enforcement, and undermine public confidence in e-commerce by deliberately inserting materially false contact data into Whois.

Significantly, it does not create a new crime or civil cause of action, and it does not target those with contact information that is either stale or outdated, and it does not penalize inadvertent or immaterial errors in Whois data, and it does not interfere in any way with domain names used for legitimate purposes.

In our testimony, we identify three initial areas that we would like to work with the Committee on clarification. Mr. Chairman

and Ranking Member Berman, we appreciate your willingness to say that there will be further work on this.

The three points are that, first, we believe it has to be made absolutely clear that providing false Whois contact data is not the exclusive way of proving willful infringement in the online environment. I don't think that's what anyone intended, but we just have to make sure that willfulness remains, as it is today, a flexible concept.

Secondly, and I believe this emphasizes Mr. Berman's point, we believe the bill should address directly the role of the U.S. Sentencing Commission to make sure that Congress's intent is fully carried out.

And third, we would apply the criminal provisions not only to those who knowingly submit false contact information, but to those who knowingly cause such information to be submitted, since registrant contact data is not always submitted directly to a registrar but often goes through an intermediary.

In sum, while some further tinkering in the language in the proposal before you today may be needed, CCDN is pleased to be here to support the legislation in principle and we commend your leadership in introducing it and look forward to working to see it enacted.

The third point is, what further steps should we consider? I don't think any of us are under any illusions that this legislation is a panacea, that ultimately we see this legislation as one element of a broader strategy to make comprehensive progress to improve the accuracy and currentness of Whois contact data. It is clear that domain name registrars, the resellers, the domain name registries have key roles to play in this area.

The reality is that today, far too many registrars and registries do far too little to screen out false contact data, don't bother to verify or spot check data, and don't even bother to respond promptly in many cases to complaints.

We all are familiar with the current framework that imposes contractual obligations to drive accessibility and accuracy. The reality is that ICANN simply has not effectively enforced them. You've heard some of the reasons today. I think there are others that we might want to discuss in Q and A.

Thanks in large part to your oversight, we do have an updated MOU with ICANN that underscores the depths of concerns of the U.S. Government on the issues of Whois accuracy and accessibility. There are a number of obligations of ICANN, and unfortunately, we've already seen one key deadline, the end of the year, pass without a strategic plan. We have another one coming up at the end of March, where we will hopefully get a solid update on what is going on with what ICANN is doing with Whois accuracy and reliability. We'll see what they have to say at that time. But if we don't hear anything, we think Congress must seriously consider stepping in.

We look forward to working with all the key participants together in a collaborative way to increase the incentives on domain name registries and registrars to demand accurate data, to take reasonable steps to verify the accuracy of such data, and in the

end, to cancel registrations of those registrants who refuse to live up to this obligation.

Thank you again for the opportunity to testify and I look forward to answering any questions that you may have.

Mr. SMITH. Thank you, Mr. Bohannon.

[The prepared statement of Mr. Bohannon follows:]

PREPARED STATEMENT OF MARK BOHANNON

c/o Smith & Metalitz LLP
Suite 825
1747 Pennsylvania Avenue, NW
Washington, DC 20006-4637
Tel: (202) 833-4198; Fax: (202) 872-0546

## Copyright Coalition on Domain Names

**PARTICIPANTS:**

American Society of Composers, Authors and Publishers (ASCAP)

Business Software Alliance (BSA)

Broadcast Music, Inc. (BMI)

Motion Picture Association of America (MPAA)

Recording Industry Association of America (RIAA)

Software and Information Industry Association (SIIA)

Time Warner

Walt Disney Company

**Counsel:**

Steven J. Metalitz
Smith & Metalitz LLP
Email: metalitz@smimetlaw.com

Ryan M. Lehning
Smith & Metalitz LLP
Email:
rlehning@smimetlaw.com

**Internet Domain Name Fraud – New Criminal and Civil Enforcement Tools**

Prepared Testimony of

**Mark Bohannon**

General Counsel and Senior Vice President Public Policy
Software & Industry Information Association (SIIA)

On Behalf of
Copyright Coalition on Domain Names

Before the

**Subcommittee on Courts, the Internet and Intellectual Property**
**Committee on the Judiciary**
**United States House of Representatives**

Washington, DC

February 4, 2004

Mark Bohannon
General Counsel and Senior Vice President Public Policy
Software & Information Industry Association (SIIA)
1090 Vermont Ave. NW, 6th Floor
Washington, DC 20005
Tel: (202) 289-7442; Fax: (202) 289-7097
Email: MBohannon@siia.net

**U.S. House Judiciary Committee**
**Subcommittee on Courts, the Internet and Intellectual Property**
**February 4, 2004**

**Summary of Testimony of Mark Bohannon, SIIA**
**on behalf of the Copyright Coalition on Domain Names**

The Copyright Coalition on Domain Names ("CCDN") is made up of leading copyright industry trade associations; performance rights organizations; and copyright-owning companies. Its focus is to maintain public access to Whois data, and improve its accuracy and reliability, as a key enforcement tool against online infringement.

- **WHOIS: Accuracy and Accessibility are Critical to E-Commerce and Accountability Online**

Access to accurate and reliable Whois data is not only important for enforcing intellectual property rights, but is also vital for consumer protection; law enforcement investigations of online crimes; and network security. The recent epidemic of "phishing" or corporate identity theft involves all these concerns, and accurate Whois data could play a critical role in preventing or investigating such frauds. All Internet users have a stake in keeping Whois data accessible and making it more accurate.

- **Proposed Legislation is a Step Forward**

The Whois database remains riddled with inaccurate data, as it was at the time of the last hearing in September, 2003. We believe the legislation on the table at this hearing takes the right approach. It targets the "bad actors" who are using the Internet to commit crimes, infringe on intellectual property rights, or commit cybersquatting. It focuses solely on those already convicted of serious crimes, or found liable for online infringements, and who also have chosen to try to hide their tracks, complicate the work of law enforcement and undermine public confidence in e-commerce by deliberately inserting materially false contact data into Whois. It would increase the punishment that online criminals who employ this evasive technique are exposed to, and would firm up the possibility of enhanced statutory damages under copyright, and of treble damages under the Lanham Act, against pirates and counterfeiters who do likewise. In these ways, the proposed legislation would take an important step in the right direction toward cleaning up the Whois database.

- **What Further Steps Should be Considered?**

This legislation must be one element of a broader strategy to make comprehensive progress on this issue of improving the accuracy and currentness of Whois contact data. Besides enacting stronger incentives for registrants to provide accurate Whois data we look forward to working with all the key participants to increase the incentives on domain name registries and registrars to demand accurate data, to take reasonable steps to verify the accuracy of the data they receive, and to cancel the registrations of registrants who refuse to live up to this obligation. Given the attention Whois received in the recently completed Memorandum of Understanding between ICANN and the Department of Commerce, we hope that ICANN will more aggressively enforce its contracts, thus enhancing the accuracy of the Whois database. Though we do not have a specific legislative proposal to put forth at this time, we do believe that this is an appropriate subject for Congressional attention to ensure that the accuracy of Whois data – especially in the generic Top Level Domains – is improved, and that public access to this important data is not curtailed.

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

Thank you for this opportunity 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, and especially, over the past few months. The September 4, 2003 hearing held by this subcommittee reinforced the importance of accurate and reliable Whois information, particularly in the context of the Department of Commerce's recent renewal of its Memorandum of Understanding with ICANN.

I am here today on behalf of 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 Time Warner and the Walt Disney Company.[1]

[1] I also serve as treasurer of the Intellectual Property Constituency (IPC), the international group organized under the auspices of the Internet Corporation for Assigned Names and Numbers (ICANN) and its Generic Names Supporting Organization (GNSO), to advise ICANN on intellectual property issues generally, including trademark as well as copyright matters. While this testimony has not been formally approved by the IPC, I believe it is generally consistent with the public policy positions that group has taken.

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 represented by participants in CCDN 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 three main questions:

- Why is real-time public access to complete and accurate Whois data essential?
- How will your proposed legislation help?
- What further steps should be considered 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 includes 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 in 2002, 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: Last fall you heard from a representative of the FBI 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."

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. Proposed Legislation is a Step Forward

It goes without saying that Whois cannot perform the critical functions I've just mentioned if the data is inaccurate, out-of-date, or otherwise unreliable. Unfortunately, despite this subcommittee's focused attention on this issue over the last few years, the Whois database remains woefully riddled with inaccuracies.

Empirical evidence showing this problem has been presented to this subcommittee before, notably with the testimony last fall of Ben Edelman of the Berkman Center for Internet & Society at Harvard University. There is little I need to add to his statistical studies and anecdotal examples. Furthermore, many of the domain names identified in the Edelman study are engaged in illegal, or suspect activity such as intellectual property infringement or cybersquatting. Law enforcement officials have repeatedly observed that those who commit crime online through the use of registered domain names routinely cover their tracks by providing false contact information for the Whois database. This includes fraudsters engaged in crimes such as "phishing" or corporate identity theft, which CCDN discussed at length in its testimony last fall.

It's time for Congress to do something about this problem, and we believe that the legislation on the table at this hearing takes the right approach. The legislation is focused and narrowly tailored. It does not create any new crime or civil cause of action; it does not target those whose registrant contact information has grown stale or outdated; it does not penalize inadvertent or immaterial errors in Whois data; and it does not interfere in any way with the activities of those who register domain names and use them for legitimate purposes. Instead, it targets the "bad actors" who are using the Internet to commit crimes, infringe on intellectual property rights, or commit cybersquatting. It focuses solely on those already convicted of serious crimes, or found liable for online infringements, and who also have chosen to try to hide their tracks, complicate the work of law enforcement and undermine public confidence in e-commerce by deliberately inserting materially false contact data into Whois. It would increase the punishment that online criminals who employ this evasive technique are exposed to, and would firm up the possibility of enhanced statutory damages under copyright, and of treble damages under the Lanham Act, against pirates and counterfeiters who do likewise. In these

ways, the legislation before you today would take an important step, and in the right direction, toward cleaning up the Whois database.

It is important to note that this would not be the first step Congress has taken in that direction. Congress has legislated forcefully against those who abuse the domain name registration system as far back as 1999, with the Anti-Cybersquatting Consumer Protection Act. Public Law 106-113; 113 Stat. 1501A-550. Indeed, Congress has acted twice more just in the past year. In the Truth in Domain Names Act, approved by this Committee and incorporated into the PROTECT Act, Public Law 108-21, title V, subtitle B, sec. 521, Congress cracked down on those who register misleading domain names for the purpose of enticing children to visit pornographic web sites. As this Committee is well aware, there has already been a successful prosecution under this statute, and that the defendant was one of the most notorious and incorrigible cybersquatters to ply his unseemly trade in cyberspace. USA v. Zuccarini, No. 03-CR-01459 (S.D.N.Y. 2003). More recently, in the CAN-SPAM Act, Congress imposed civil and criminal liability on persons who fraudulently register domain names and use them as a launching pad for illegal and invasive unsolicited commercial e-mail. Public Law 108-187, sec. 4, sec. 7. By enacting legislation based on the bill before you today, the 108th Congress would provide a strong incentive for all registrants to provide accurate and up–to-date contact data, as they are already required to do.

As the Subcommittee moves forward to marking up this bill and preparing a report, we think it should be made absolutely clear that providing false contact data in connection with a domain name used to commit a felony is not the exclusive way of proving that copyright or trademark has been infringed willfully in the online environment. Willfulness is and must

remain a flexible concept, and the subcommittee should make sure that this legislation cannot be misread to undercut this. Similarly, the subcommittee should consider whether the legislation should specifically address the role of the U. S. Sentencing Commission in ensuring that Congress' intent – that those who abuse the domain name registration system in the course of criminal activity must receive stiffer punishment – is fully carried out.

The Subcommittee might also consider extending the criminal provisions not only to those who knowingly submit false contact information, but to those who knowingly cause such information to be submitted. This would recognize that in a number of business models, registrant contact data is not submitted directly to a registrar but goes through an intermediary.

In sum, while some further tinkering with the language in the proposal before you today may be needed, CCDN is pleased to support this legislation in principle. We commend your leadership in introducing it and look forward to working with the subcommittee and your colleagues to see it enacted.

## III. What Further Steps Should Be Considered?

While CCDN believes the enactment of the legislation under consideration would mark an important step forward, we are under no illusions that it would provide a panacea. It will discourage domain name registrants, especially those who are contemplating illegal or fraudulent activities online, from providing false contact data, but it certainly will not end this practice.

Ultimately, this legislation must be one element of a broader strategy to make comprehensive progress on this issue of improving the accuracy and currentness of Whois contact data. Domain name registrars and their resellers, who actually sell registrations at retail, and the domain name registries, which maintain the master lists of registrations within a particular Top Level Domain, such as .com, .net or .org., have key roles to play.

Both registrars and registries have contractual obligations to ICANN – the Internet Corporation for Assigned Names and Numbers – that address the accessibility and accuracy of Whois data. But, as you may recall from our previous testimony on this subject, we believe that while ICANN has made some efforts to use its contractual authority to correct this problem, it has not done nearly enough.

The current stance of ICANN on Whois has not changed substantially over the past few months. 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 not been consistently and effectively enforced by the one entity with clear authority to enforce them: ICANN.

Thanks in great part to the oversight activities of this Subcommittee, the Department of Commerce, in the revised Memorandum of Understanding with ICANN which it concluded last September, underscored the depth of concern of the U.S. government on issues of Whois accuracy and accessibility. Specifically, in section II.C.10 of the MOU, DOC instructed ICANN to "[c]ontinue to assess the operation of Whois databases and to implement measures to secure improved accuracy of Whois data." ICANN is supposed to report on its progress in this area as well as others every six months, beginning in March. ICANN is also obligated to "augment its corporate compliance program," including its efforts to "audit material contracts for compliance." Certainly those contracts include the agreements with registrars and registries, and the audits should address compliance with the Whois obligations of those agreements.

It is far too soon to tell whether the new features of the revised MOU are having the desired effect. We note that the MOU set a deadline for ICANN to develop a strategic plan to address a number of issues, including contract compliance. That deadline was December 31, 2003. That day came and went without any public release from ICANN. This does not bode well for the host of tasks and deadlines that ICANN is yet obligated to meet.

Copyright and trademark owners, and the organizations that represent them, support ICANN, and we continue to participate actively in the many and manifold ICANN policy development processes, including those related to Whois. Much can be accomplished through dialogue in the ICANN framework, 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 this continued support and engagement.

We are under no illusions here; we know that it will not be easy to overcome ICANN's long-standing reluctance to step up to these issues. But we hope that, through the oversight of this Subcommittee and the revitalized attention of the Department of Commerce to these issues, ICANN can be strongly encouraged to carry out these MOU obligations fully and comprehensively. This would be in the best interests of the world Internet community that ICANN is institutionally pledged to serve.

While there is much more that could be said about ICANN, this hearing is not about ICANN, but primarily about how Congress can effectively legislate to improve Whois and thus to bring greater transparency and accountability to the domain name system and to the Internet as a whole. In this regard, besides enacting stronger incentives for registrants to provide accurate Whois data we look forward to working with all the key participants to increase the incentives on domain name registries and registrars to demand accurate data, to take reasonable steps to verify the accuracy of the data they receive, and to cancel the registrations of registrants who refuse to live up to this obligation.

It is obvious that today, far 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.

We do not have a specific legislative proposal to put forth at this time, but we do believe that this is an appropriate subject for Congressional attention. We recognize the international aspects of the domain name registration system, which may make it more difficult to craft an effective legislative solution. And we acknowledge the important role that ICANN must and should play, a role for which additional legislative authority may not be needed. However, just as Congress was not deterred from legislating against abusive domain name registration practices of pornographers and spammers, it should not hesitate to take the necessary steps to ensure that the accuracy of Whois data – especially in the generic Top Level Domains – is improved, and that public access to this important data is not curtailed. In the meantime, we look forward to working with the subcommittee to refine and perfect the legislative proposal under consideration today.

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

Mr. SMITH. It's nice for those of us who are Members of this Subcommittee to have a panel of four witnesses basically in agreement on almost every point, and that's a rare thing sometimes.

Mr. Trainer, let me address my first question to you, and perhaps to Mr. Wesson, as well, and thank you. You made a half-a-dozen suggestions on provisions that we ought to include in the bill, and to me, they're good suggestions and we'll look at them seriously.

My question, Mr. Trainer and Mr. Wesson, is this. We really have two problems with registrars. One, we have the problem that either they aren't or won't verify the information they're given. Maybe they don't have the incentive. For whatever reason, the information is not being verified by the registrars.

The other half of the problem, and I think you noted this, Mr. Trainer, is that they're not able to verify the information. They just don't have the tools they need to verify what they're given. How would you solve that problem with the registrars?

Mr. TRAINER. Well, one of the things that I think I noted, and hopefully correctly, is in reviewing the Registrar Accreditation Agreement, frankly, I felt that there was a lack of obligation, affirmative obligation, on the registrars to truly act, and if they didn't, where was the liability on the registrars if they didn't act?

I think Mr. Wesson has raised a very interesting issue with regard to maybe there's, if not a full solution, a partial solution, and that is technology. Given the fact that we have many companies out there every day trying to come up with new and better things, it's hard to believe that there's not someone out there that can write a software program certainly to identify some of the basic problems that we have found through our Members. So I think it's really, as he said, if they felt that there was no solution out there, why would they bother to take the next step?

So I think we have to put a little more pressure on the registrars and we're more than happy to work with you and your colleagues here on the panel with regard to the way in which we may do that with regard to registrars.

Mr. SMITH. Okay. Thank you, Mr. Trainer.

Mr. Wesson?

Mr. WESSON. Certainly, the registrars didn't know that there was a way to do this until about 18 months ago, and it is difficult for any business that's on the Internet that needs to be able to validate address, telephone, postal information for 200-plus countries where all of your customers might reside, and we don't want to leave a space so that people can constantly register in one place and you know that it's going to be fraudulent because we can't perform analysis from that particular country.

As far as having the registrars participate in a program like this, one would be cost, and two, that there's nothing right now that, as a registrar, as long as you're paid, then what's the problem? There's no incentive. There's no business reason to require accurate information.

Mr. SMITH. Okay. Thank you, Mr. Wesson.

Although it was Mr. Evans, I think, that gave examples a while ago that there are just some common sense types of information

that were given that were still being accepted without any question, and that was disappointing, as well.

Mr. Evans, let me ask you about ICANN. I think you pointed out that, or you were disappointed, as I am, that ICANN really has not taken very many steps. In fact, I think they've really only gone after one registrar when it comes to supplying inaccurate information and that doesn't seem to me to be a particularly good faith effort to try to clean up the system itself.

Mr. Bohannon, you pointed out that we're getting the first report from the MOU at the end of March. I think it's due March 31, and I'm not particularly hopeful about what that may or may not show us.

But in any case, my question to Mr. Evans and Mr. Bohannon is this. What is your opinion so far of ICANN's performance and what specifically should we do to try to persuade or make them do a better job of providing consumers and attorneys and businesses with more accurate Whois data. Mr. Evans?

Mr. EVANS. Well, in my opinion, ICANN's progress today is typical. For people who have followed the activities of ICANN, I think while they have begun some type of process with regards to Whois accuracy, it is one that is mired in discussing the process rather than one in coming up with concrete results and solutions to a problem. So I would say it's typical and it's mired in squabbling over process rather than actually moving forward, which tends to bog a lot of ICANN's progress down.

With regards to what this Subcommittee can do to assist ICANN is I'm not so sure that you all can do anything to assist ICANN, but you can give tools to trademark owners, intellectual property owners, to be able to go to the registrars or the individuals and/or companies that participate in these activities and reckon from them the just penalty for their unfortunate activities.

Mr. SMITH. Thank you, Mr. Evans.

Mr. Bohannon?

Mr. BOHANNON. Mr. Chairman, I want to make sure I answer the question as clearly as I can, but I think it's important to distinguish between the overall mission of ICANN and the particular role of ICANN with regard to Whois issues.

With regard to the first, CCDN has actually not taken a position on the overall mission of ICANN. I can say for my own personal association's point of view, we continue to believe that ICANN remains the most viable way of avoiding complete Government regulation of the Internet in terms of the domain name registration process, and we think it is generally headed in the right direction with regard to that.

With regard to the second question about what it is doing to enforce the contracts and make sure that Whois data is available, I would have to give it a grade of D or D-minus. I think we're talking about some really serious problems here, some of which have to do with elements of the accreditation agreement, some of which have to do with the practical economics, some of which have to do with time commitments, priorities. We're simply not seeing any pressure to say to the registrars, this is something you're obligated to do. What are you doing about it? What are you doing to hold them accountable? So that's the bottom line on that.

Mr. SMITH. Thank you, Mr. Bohannon.

The gentleman from California, Mr. Berman, is recognized for his questions.

Mr. BERMAN. Well, thank you, Mr. Chairman.

This issue of the feasibility of the registrars playing a greater role in obtaining accuracy and the incentive, incentives to do it, how do the registrars normally get paid? I assume by credit card in most cases. Is that a reasonable assumption?

Mr. WESSON. That's correct, sir.

Mr. BERMAN. I mean, they certainly have an incentive to do something to ensure that the credit card they're being given is that person's credit card and that payment will be made. What do they do to determine that the person registering for the domain name is providing a valid credit card which will be paid?

Mr. BOHANNON. There's actually no way to determine the association of the contact information with the cardholder, and that's a global problem. In the United States, a registrar will simply charge the card and hopefully use some of the security features available in processing that card, and then if the card is not—if the transaction is not disputed by the individual that owns the card, they get to keep the money.

Mr. BERMAN. When you go through checking out the person who owns that card, does that provide information that the registrar could then include on the—in terms of domain name information?

Mr. WESSON. No, sir. There's no way to correlate cardholders with any kind of registrant information.

Mr. BERMAN. But there would be a way, at least in some cases, to assume the cardholder would know where to get the accurate information about the domain name owner.

Mr. WESSON. Actually, it's very difficult and there's no capabilities as credit card processors to retrieve the information about the credit card holder. So we can't even contact them——

Mr. BERMAN. You're basically checking with a credit card company and they're saying this card is a valid card and—and if the money is paid and no dispute is sent about the bill, that's—all you have is that it was valid.

Mr. WESSON. Yes, sir. This is how credit card transactions work generally over the Internet.

Mr. BERMAN. Some people argue that this legislation, and more particularly, some of the future amendments that you're suggesting and we're contemplating, encroaches on an individual's legitimate expectation of privacy. Mr. Bohannon, how would you respond to that? Are we proposing and contemplating measures which would be invasive of legitimate privacy concerns?

Mr. BOHANNON. I think, Mr. Berman, the privacy question is an important one, but I think it's also a red herring in this area. I think—our view is that, in fact, accurate, up-to-date, reliable Whois will do more to promote privacy than the existing system since, as we know from the studies that most of the misinformation—those registrations that have bad information are, in fact, those engaging in identity theft, fraud, copyright infringement, trademark infringement, and that, in fact, an accurate Whois will go far toward promoting privacy. That is, if someone is, in fact, engaging in identity

theft, taking your information, we have a better chance of tracking that person down or that entity down than we did before.

I think that with regard to those websites that may be registered by individuals, which I think is probably the more sensitive issue, in principle, we work with intermediaries and proxy services who can, in fact, keep that information, and so long as it is accurate and readily available, we have no problem with that.

I think that the expectation of privacy question, when you're talking about a domain name—not an e-mail address but a domain name—is really very, very different than, I think—that it really doesn't raise the issues that you're talking about.

Mr. BERMAN. It's like applying for a business permit in the city. There are certainly expectations and you want to have a license to do business, you provide certain information about the place and ownership of the business.

On the other side of the coin, for people who seek domain names in order to—let's put it in the most important, say, first amendment areas. They want to send a political message and they want to maintain anonymity because they're fearful of repercussions. I mean, this came up in the non-digital world many years ago in the case about the membership lists of the NAACP and things like that. Is there anything here that would be intrusive of some fundamental right to association and——

Mr. BOHANNON. Not at all. I think because the bill does not create a new crime for providing, knowingly providing or causing to provide, hopefully, misinformation, we're really talking about a class of people that have already been, in fact, found to have been guilty of a Federal crime. So I don't think we're talking about creating a new crime here that would raise the kind of issues that you talk about.

Mr. BERMAN. But are any of you suggesting that we alter this bill to create a new crime on the—are you all comfortable with the approach where essentially this becomes an additional liability or an additional sentence, either civil or criminal liability, for the posting of a false domain name? Do you find that to be the best way to approach this issue?

Mr. EVANS. I certainly think you avoid some of the privacy concerns, because unless you're using the domain name to violate a crime that already exists and you have in association with that supplied the false and misleading information, you don't—you're not guilty of anything. So if you are perhaps an individual that wants to rail against a particular point of view and are concerned about your privacy, you never fall within the legislation at all.

Mr. BERMAN. If what you do isn't a substantive crime——

Mr. EVANS. That's correct.

Mr. BERMAN.—providing false information will not——

Mr. EVANS. That's correct.

Mr. SMITH. Thank you, Mr. Berman.

The gentleman from Virginia, Mr. Goodlatte, is recognized for his questions.

Mr. GOODLATTE. Thank you, Mr. Chairman. I very much appreciate your holding a hearing on this very important subject. I have an opening statement I'd ask be made a part of the record.

Mr. SMITH. Without objection, the opening statement will be made a part of the record.

[The prepared statement of Mr. Goodlatte follows in the Appendix]

Mr. GOODLATTE. Thank you. Mr. Trainer, can you comment on the global scope of this problem? Mr. Wesson testified that the registration of Internet domain names is a global undertaking. Registrars in France can sell domain names to U.S. entities as well as to entities from other countries. What can we do in America to ensure that registrars in other countries require accurate registration information?

Mr. TRAINER. I'm not sure that I'm the best person to be able to respond to that one——

Mr. GOODLATTE. We'll give anybody else that wants to jump in an opportunity.

Mr. TRAINER.—but given that our members and my interaction with our members is really to deal with the counterfeiting/piracy issues, certainly it is important globally because they are—the multinationals are active globally.

So I think—I find it very interesting, what Mr. Wesson has raised with regard to possible technological fixes. I think, again, what we talked about earlier, about possibly looking at this and placing more burden on the registrars to actually have a more affirmative role here, to look at what they're getting and verifying what they're getting rather than sitting back and simply accepting credit cards and the cash payments. But yes, it's an issue that I think would affect our members around the world.

Mr. GOODLATTE. Anybody else want to jump in on that? Mr. Wesson?

Mr. WESSON. I believe that the only—the only entity that really has any oversight over them would be ICANN. I don't know how effective they would be or if they would even have the capability to do anything about it, but——

Mr. GOODLATTE. Is ICANN attempting to put forth any protocols on what steps should be taken to assure accurate information when they set these up?

Mr. EVANS. I think ICANN is spending a lot of time talking about the process of how they should go about doing that, but I don't think they've offered any solutions.

And I would also point out that, you know, the Internet is not something that is so different from the rest of industries that exist in the brick-and-mortar world that we should worry about the global implications. There are many international corporations that do business in the United States and are subject to our laws. So I think that putting forth and promulgating statutory solutions for businesses that choose to do business in the United States is the right step if we can't get solutions elsewhere. And the fact that there may be international institutions involved, they accept the benefits of doing business in this country and they will have to assume the risk, as well.

Mr. GOODLATTE. Thank you. Mr. Wesson, I believe that technology such as yours will go a long way toward determining the accuracy of domain registration information. However, as you point out in your testimony, these types of technologies can only be lever-

aged when domain name registrars have the incentives to use the information derived from the technologies to make registration information accurate.

In your opinion, what would be the most effective way to encourage these registrars to ensure the accuracy of domain name registration information?

Mr. WESSON. That's a very good question, sir, and unfortunately, I don't have an answer for you. I do not know, and I have worked at some length to convince registrars that it is in their best interest and in the best interest of the Internet community that this job be undertaken, and I was unable to convince them. I do not know the best methodology to do that.

Mr. GOODLATTE. Anybody else have any thoughts on that subject? Let me ask Mr. Bohannon or Mr. Evans, what additional steps do you believe need to be taken to encourage domain name registrants to provide—and registrars to ensure accurate registration information?

Mr. BOHANNON. Mr. Goodlatte, good to see you. Thank you for coming today. I like your question. In our testimony, we're very clear that we see this bill not as a panacea but as one step toward a comprehensive effort to improve accuracy. Clearly, we've got to focus on the registries, the resellers, and the registrars.

We don't come with a proposal, but we look forward to working with this Committee and all the stakeholders to sit down and say, we've got to come up with some real incentives for the registries and the registrars to demand accurate data, to take reasonable steps to verify, and in the end, to cancel registrations for those registrants who aren't living up to what they're supposed to be doing.

We don't come with preconceived notions, but we've got to figure out a way, with the oversight and leadership of this Subcommittee, to get all the key players together to figure out how we can do that together.

Mr. GOODLATTE. Thank you.

Mr. EVANS. Just let me echo Mr. Bohannon's comments. We look forward to working with this Subcommittee and its staff to help craft solutions. We see that the pending legislation is a move in the right direction and we are hopeful that, working with the staff and the Subcommittee, that we can together collectively come up with creative solutions that will move us forward in order to solve the problem that I think we all have identified.

Mr. GOODLATTE. Very good. Thank you, Mr. Chairman.

Mr. SMITH. Thank you, Mr. Goodlatte, and thank all the witnesses today for their testimony. As I mentioned at the outset, it's been very, very useful and we will, I suspect, adapt a lot of the suggestions that you all made for additional provisions in the bill. You are welcome to continue your comments between now and markup, but we very much appreciate your input today. Thank you all.

We stand adjourned.

[Whereupon, at 11:04 a.m., the Subcommittee was adjourned.]

# APPENDIX

## MATERIAL SUBMITTED FOR THE HEARING RECORD

### PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. Chairman, thank you for holding this important legislative hearing regarding the ongoing problem that fraudulent domain name registration information poses for the safety and fairness of the Internet.

"WhoIs" databases consist of the names, addresses, email addresses, and phone numbers of domain name registrants. While many Internet users wish to maintain anonymity, this information is crucial to law enforcement officers trying to locate and detain criminals who use the Internet to perpetrate crimes, including those who falsify their identities to perpetrate crimes against children.

In addition, in the digital age, one of the most crucial hurdles in enforcing intellectual property rights is to determine the identities and locations of the infringers. Accurate "WhoIs" data enables IP owners to find violators quickly in order to defend their property rights. WhoIs data is also essential to finding perpetrators and alerting potential online targets regarding network attacks.

With the advent of additional top-level domain names and due to the stiff competition among registrars in the registration of these new domain names, some argue that currently there is an incentive for registrars to turn a blind eye to false information or to overlook many of the requirements to monitor and keep track of accurate "WhoIs" data. Further complicating the problem is the fact that there are relatively few enforcement tools to punish those that provide fraudulent domain name registration information.

H.R. 3754, the "Fraudulent Online Identity Sanctions Act," is one additional arrow in the quivers of law enforcement officials, intellectual property owners, network security specialists and consumers. This bill will provide greater penalties for providing fraudulent contact information to a domain name registry, when the perpetrator uses the online location in connection with trademark and copyright infringement, or in connection with federal criminal offenses. I applaud the introduction of this legislation and look forward to hearing from the expert witnesses on the merits of the bill.

Thank you again for holding this important hearing.

---

To the honorable Chairman Lamar Smith,

The undersigned registrars commend the Subcommittee for highlighting the issue of Whois accuracy. It is a complex topic of importance to governments, intellectual property interests, the Internet sectors, and individuals and organizations registering domain names. Because Whois data must be available to third parties under current ICANN policies, both privacy and accuracy concerns are involved. Registrars respectfully submit the information below to round out the various issues related to data accuracy.

*The Bill*

The current draft of the bill seems to impose additional liability on persons who knowingly provide false data when registering a domain name—the "registrants" or their representatives acting on their behalf. While it appears to target bad actors who have already been found by a court to have violated provisions of the Lanham Act and the Copyright Act, to the extent that the bill would create liability for registrars, we would favor textual clarification of that point. Based on an understanding that the bill does not create liability for registrars, we are not taking a

position to oppose the bill and, in fact, we support the bill's overall goal of improving data accuracy.

We look forward to continuing to work with your Subcommittee on this bill. If upon closer examination, issues of concern are noted, we would respectfully request the opportunities to work with you and your staff on suggestions and amendments to this language.

*What is the Whois*

Essentially, the Whois is a database of contact information about domain name registrants. It is accessed through the websites of registrars or registries, as well as through technical means by the registrars and registries, themselves. Due to vigorous competition in the registrar market, the provision of Whois data may vary among different registries - the operators that maintain the list of available domain names within their extension - and registrars - the organizations, such as the undersigned, that maintain contact with the client and act as the technical interface to the registry on the client's behalf.

Currently for the generic top-level domains (gTLDs) .com and .net, the registry holds a 'thin' Whois, which has a limited subset of the Whois information in the registrars' Whois database (registrar name, name servers and expiry date). The registrar for each domain name holds the 'thick' Whois, which contains more detailed information. A lookup for the same name at the registrar will also include details of the registrant, administrative, technical and billing contacts.

In the case of the country code top-level domains (ccTLDs) such as .uk for the United Kingdom and .de for Germany, and the new gTLDs such as .biz and .info, both the registries and registrars generally hold the 'thick' Whois. However, the level of detail kept by the registries will vary. While gTLDs hold full information, some ccTLDs have no information immediately available. The ccTLDs' rules are often shaped by their jurisdictions' privacy and other laws.

Over the last couple of years there has been a debate within ICANN (the domain name oversight body) and among various governments over Whois information, with intellectual property owners on one side arguing for greater access and more Whois details, and privacy advocates arguing for greater privacy protection of and less publicly available personal data. Full and accessible Whois details are important to IP owners for the monitoring of trademark infringements and to determine whether a particular individual has developed a pattern of cyber squatting activities. Consumers have grown increasing more concerned about the privacy of their personal contact information as they are increasingly victimized by bad actors, which include spammers, fraudsters, and stalkers who mine the Whois database for unscrupulous purposes.

The broad interest in Whois privacy protection and accuracy has prompted a policy development process within ICANN. ICANN's counsel wrote a report regarding the issues and processes surrounding Whois and privacy. The GNSO Council reviewed the report and launched three task forces, which are currently working with the full support of registrars on these matters. The goal of the process is to identify the experiences and interests of the relevant stakeholders - providers, users, and consumers - and arrive at a technical and policy solution that balances these interests and concerns. The results and education from these processes can feed into improved ICANN policies, helping to hasten a solution.

*Current Safeguards*

Even while working through this process, various registrars already use accuracy processes, including:

- updating a registrant's data upon notice;
- taking down a registration if inaccurate information is not cured in a timely manner;
- sending notifications to all customers reminding them to update their data or face the risk of the registration being taken down or put on hold; and
- checking credit cards prior to registration to minimize fraud.

Despite such precautions, the savvy cyber squatter can sneak through. He can use stolen credit cards or credit cards that are in good standing; provide apparently valid information, and update it to other seemingly valid addresses when prompted. But, credit card companies' privacy rules prohibit use of their data for other pur-

poses, such as Whois verification. There simply is no guarantee that persons intent on registering a domain name with invalid data can be stopped and anyone who offers automated filters cannot claim to have found a comprehensive solution.

*Privacy*

What seems to help, actually, is increased privacy protection on the Whois database. Many individuals and even corporations today seek greater privacy - to avoid spam, to safeguard addresses, and for many other valid reasons (illustrated below). Recent legal cases illustrate the great harm caused by the unscrupulous taking and use of openly available Whois data.

Such efforts to increase privacy should not be confused with complete anonymity, however. A responsible registrar that increases its customers' privacy would also be able to provide legitimate interests, such as trademark holders and law enforcement, with access to the information they need. The benefit for all parties is that greater privacy would encourage registrants, who are justifiably concerned about unfettered free-for-all access to their emails or phone numbers, to provide accurate data if it is protected.

While we do not oppose this bill, subject to the statements in our opening comments, we believe that its goals would be strengthened if paired with legislation facilitating greater privacy.

*Illustration of Fraud Problems Associated with Mining the Whois Database*

Registrants have been hit by fraudulent, abusive and annoying solicitations directed at their contact information mined from the public Whois database. Below is only a sample of the many instances in which scam companies have mined the Whois database.

The issues span the gamut from outright fraud to stealing credit card information, to fear-instilling "renewal" notices, to annoying and unwanted spam solicitations. Few instances of Whois abuse involve simple, non-deceptive transfer solicitations. Too many registrants have fallen victim to credit card schemes, or have paid registration fees to unscrupulous marketers who pass themselves off as the registrar, using deceptive marketing techniques, only later to learn that they have paid a non-refundable fee to a shady company.

Highlights (or more accurately, low points) include:

- *Credit Card Fraud*: Perpetrators of a credit card fraud scheme mined the automated Whois database to obtain a registrar's customer contacts and sent deceptive "renewal" notices to its customers. There is reason to believe that tens or hundreds of thousands of customers received the fraudulent email. There was no way of knowing how many of the customers fell prey to the scam and provided their credit card information, but suspect that the number may be in the hundreds. The dollar value of the harm inflicted on the customers could range from the hundreds of thousands of dollars to the millions of dollars, depending on whether their credit cards were charged prior to cancellation, and on whether the above scam is a part of a larger identity theft ring. The perpetrators of the fraud repeatedly circumvented efforts to shut down the site's operation and re-launched it with the same or different hosting providers.
    - These types of scams, known as "phishing," are increasing in popularity among fraudsters, and are particularly difficult to locate and stop, especially given the global nature of the Internet.
- *Renewal Scams*: Another scheme relies upon Whois information that has been mined to inundate registrants with misleading "renewal" solicitations. These solicitations do not explain that registrants who accept the solicitation will actually be transferring their domain name registrations away from their current registrar. To the contrary, the solicitations are designed to induce customers to falsely believe that the solicitations were sent by or on behalf of their registrar, and/or that they were required to "renew" their registrations with the sender of the notices or they will risk losing the ability to use their domain names altogether.
    - Customers may believe they are simply "renewing" their existing registrations and unwittingly pay and transfer their domain names. In many

instances, customers who seek to unwind these transactions are unable to recover their money.

- Customers induced to "renew" their registrations have lost email records, contact directories, and other benefits attached to their accounts.
- Other customers, believing that the reseller is affiliated with their registrar complained that their privacy has been violated by the aggressive solicitation campaign and even erroneously accused their registrar of selling their contact information.

Sincerely,

Network Solutions, LLC
Bulk Register
Register.com
Melbourne IT

Cc: Ranking Democrat Berman

---

February 13, 2004

The Honorable Lamar Smith
Chairman
U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, the Internet
and Intellectual Property
B-351-A Rayburn Building
Washington, D.C. 20515

Re: Fraudulent Online Identity Sanctions Act

Dear Chairman Smith,

Network Solutions, LLC ("Network Solutions") submits this letter to the Subcommittee on Courts, the Internet and Intellectual Property ("Subcommittee") concerning proposed H.R. 3754 otherwise cited as the Fraudulent Online Identity Sanctions Act ("FOISA"). Network Solutions writes to address concerns raised under the current version of the draft bill.

The consensus of the bill's proponents, as reflected in their testimony before the Subcommittee on February 4, 2004, seems to support a narrow interpretation of the bill in terms of criminal or civil liability. Network Solutions would agree with this interpretation of the bill. Certain provisions of the bill, however, raise concern that prosecutors or intellectual property rights holders may nevertheless seek to hold registrars liable under its provisions should the bill become law. The bill would add an additional provision to Section 35 of the Trademark Act of 1946 that states, "(e) In a case of a violation referred to in this section, occurring at or in connection with an online location, the violation shall be considered to be willful for purposes of this section if the violator, or a person acting in concert with the violator, knowingly provided material and misleading false contact information to a domain name registrar, domain name registry, or other domain name registration authority in registering a domain name used in connection with the online location, or in maintaining or renewing such registration." The bill also proposes an amendment to the Copyright Act containing similar provisions.

In carrying out their ICANN accredited functions, domain name registrars provide contact information to registries when registering domain names. Registrars do so at the time of an initial domain name registration and whenever registrants update their contact information—during the maintenance or at the renewal of said domain name registration.

Additionally, as noted in prior testimony before the Subcommittee, registrars are obligated under their agreements with ICANN to investigate complaints of inaccurate Whois data and to take action, if warranted, in response to those complaints. The receipt by registrars of complaints about inaccurate Whois data could raise a question of notice, albeit inconsistent with the intent of this bill, that could be put forward by parties seeking to impose liability on registrars. Although such a construction would be beyond the bounds of a reasonable interpretation of this bill, Network Solutions suggests that such claims can be anticipated.

As noted in the testimony of Mr. Mark Bohannon of the Copyright Coalition on Domain Names, "[t]he legislation is focused and narrowly tailored. It does not create any new crime or civil cause of action; it does not target those whose registrant contact information has grown stale or outdated; it does not penalize inadvertent or immaterial errors in Whois data; and it does not interfere in any way with the activities of those who register domain names and use them for legitimate purposes. Instead, it targets the 'bad actors' who are using the Internet to commit crimes, infringe on intellectual property rights, or commit cybersquatting. It focuses solely on those already convicted of serious crimes, or found liable for online infringements, and who also have chosen to try to hide their tracks, complicate the work of law enforcement and undermine public confidence in e-commerce by deliberately inserting materially false contact data into Whois."

Since proponents of the bill believe that the provisions are narrowly tailored to target "bad actors" who have violated the Trademark Act or Copyright Act, inclusion of an explicit exemption for ICANN accredited registrars and registries, when acting in the normal course of their accredited functions, would be consistent with the intent of the bill and would add clarity to relieve the above stated concerns held by registrars under the current draft version of the bill.

Network Solutions would be happy to provide proposed language to be included in the bill and would welcome the opportunity to further discuss this matter at your convenience.

Sincerely,

X

Brian Cute
Director of Policy
Network Solutions, LLC

Cc: Ranking Minority Leader Berman