AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ICANN AND THE WHOIS DATABASE: PROVIDING ACCESS TO PROTECT CONSUMERS FROM PHISHING

HEARING

BEFORE THE

SUBCOMMITTEE ON
FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 18, 2006

Printed for the use of the Committee on Financial Services

Serial No. 109–108

U.S. GOVERNMENT PRINTING OFFICE
31–537 PDF WASHINGTON : 2007

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
RICHARD H. BAKER, Louisiana
DEBORAH PRYCE, Ohio
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LaTOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, Jr., North Carolina
JUDY BIGGERT, Illinois
CHRISTOPHER SHAYS, Connecticut
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona
JIM GERLACH, Pennsylvania
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
MICHAEL G. FITZPATRICK, Pennsylvania
GEOFF DAVIS, Kentucky
PATRICK T. McHENRY, North Carolina
CAMPBELL, JOHN, California

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, Jr., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
CAROLYN McCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
MELISSA L. BEAN, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
GWEN MOORE, Wisconsin,

BERNARD SANDERS, Vermont

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

SPENCER BACHUS, Alabama, *Chairman*

WALTER B. JONES, JR., North Carolina, *Vice Chairman*
RICHARD H. BAKER, Louisiana
MICHAEL N. CASTLE, Delaware
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SUE W. KELLY, New York
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
JUDY BIGGERT, Illinois
VITO FOSSELLA, New York
GARY G. MILLER, California
PATRICK J. TIBERI, Ohio
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
RICK RENZI, Arizona
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
PATRICK T. MCHENRY, North Carolina
MICHAEL G. OXLEY, Ohio
BERNARD SANDERS, Vermont
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
LUIS V. GUTIERREZ, Illinois
DENNIS MOORE, Kansas
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
JOSEPH CROWLEY, New York
STEVE ISRAEL, New York
CAROLYN MCCARTHY, New York
JOE BACA, California
AL GREEN, Texas
GWEN MOORE, Wisconsin
WM. LACY CLAY, Missouri
JIM MATHESON, Utah
BARNEY FRANK, Massachusetts

CONTENTS

ICANN AND THE WHOIS DATABASE: PROVIDING ACCESS TO PROTECT CONSUMERS FROM PHISHING

Tuesday, July 18, 2006

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 2128, Rayburn House Office Building, Hon. Spencer Bachus [chairman of the subcommittee] presiding.

Present: Representatives Bachus, Kelly, Gillmore, Hensarling, Pearce, Maloney, Moore of Kansas, Baca, and Clay.

Chairman BACHUS. Good morning. The subcommittee will come to order. I have, in the interest of time, submitted a written statement for the record, but I'm going to shorten my opening statement.

At today's hearing, we will focus on proposals before the Internet Corporation for Assigned Names and Numbers, ICANN, that would limit the public's access to domain name registrants' contact information via the WHOIS database.

This would put many long-standing and valuable uses of this data off limits and can make it difficult for law enforcement and financial institutions to identify, block, shut down, and in some cases, prosecute, the perpetrators of online financial fraud.

It has always been ICANN's policy to collect contact information from registrants of Internet domain names and make it available to the public.

This policy helps to promote accountability online, since consumers, financial regulators, and others seeking to determine who or what entity is responsible for a particular Web site or other online location can obtain this data through a service called WHOIS.

Financial institutions, which are the focus of this hearing, use WHOIS data to combat identity theft and account fraud, particularly as it relates to phishing.

The financial services industry is currently battling phishing scams at an unprecedented level. In May 2006, the Anti-Phishing Working Group, which is comprised of financial institutions, ISP's, and law enforcement, reported merely 12,000 phishing sites, which on average remained online for 5 days. These sites hijacked the brands of 137 companies in an attempt to fraudulently gain access to sensitive consumer information.

Notwithstanding the critically essential and legitimate uses of the WHOIS database, ICANN is actively considering a policy change to restrict WHOIS data to those who resolve, "technical issues." If this change is adopted, public access to most of the data now in the WHOIS database would be denied, perhaps including data as fundamental as the name of the domain name registrant.

I am concerned such proposals limiting the use of the information for resolving technical issues will make it difficult for financial institutions to respond effectively to identity theft and phishing attempts.

Timely response to these attacks and identity theft is critical to protect financial institutions as well as innocent customers who are most often unaware of their victimization.

In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Such uses of WHOIS data would become slower, more difficult and expensive, if not impossible, were ICANN to adopt the policy now being proposed.

I am hopeful that today's hearing will enlighten and inform the committee as we address what could be a serious setback for attempts to combat identity theft and fraudulent financial transactions.

Let me just say the bottom line is that continued full access to WHOIS data, I believe, is an important tool in the fight against fraudulent activity against consumers online.

Mr. Moore, I'll recognize you for an opening statement.

Mr. MOORE OF KANSAS. Thank you, Mr. Chairman, for convening this hearing. I do not have an opening statement. I look forward to the statements of the witnesses. Thank you.

Chairman BACHUS. Let me just say that I want to take this opportunity to thank you for your participation on the committee. You are a valuable member and discharge your duties in a very professional way. I very much value your advice and input.

Mr. Hensarling?

Mr. HENSARLING. [Off microphone]

Chairman BACHUS. Thank you, Mr. Hensarling. I could very well say the same thing about you. I appreciate your participation in the hearing.

Our first panel is made up of Mr. John Kneuer, Acting Assistant Secretary of Commerce for Communications and Information, and Administrator of National Telecommunications and Information Administration, U.S. Department of Commerce, and Ms. Eileen Harrington, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission.

I have reviewed both of your resumes, and they were both very impressive. We welcome both of you to the hearing.

Mr. Kneuer, we will start with your testimony.

STATEMENT OF JOHN M.R. KNEUER, ACTING ASSISTANT SECRETARY OF COMMERCE FOR COMMUNICATIONS AND INFORMATION AND ADMINISTRATOR OF NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Mr. KNEUER. Thank you, Chairman Bachus, and members of the committee. I am pleased to have this opportunity to address recent developments related to ICANN and the WHOIS databases, and the role of the Department of Commerce in this critical area.

The Department strongly supports continued access to an accurate, searchable, and publicly available WHOIS database. This data is critical to meeting a variety of public policy objectives, including law enforcement and consumer protection.

We have been proactively advocating this position at the meetings of ICANN and elsewhere.

Under the Memorandum of Understanding (MOU) between the Department and ICANN, ICANN has agreed to continue to assess the operation of the WHOIS databases and to implement measures to ensure secured improved accuracy of WHOIS data.

In accordance with those specific provisions, ICANN has published three annual reports that provide information on community experiences with the WHOIS database's problems reporting system.

While ICANN has full oversight of the WHOIS databases, there has been some concern about ICANN's generic name supporting organization, the GNSO, and the policy development process it has initiated, which among other things seeks to re-define the purpose of WHOIS data.

In April 2006, the GNSO Council voted in favor of a new definition of the purpose of WHOIS data that is, "To resolve issues related to the configuration of the records associated with the domain name within a DNS name server."

This definition is considered by many, including the U.S. Government, as a narrow technical definition.

We have been working within the ICANN process to address this concern.

It is important to understand that this definition reflects only the views of the GNSO Council, and it does not currently reflect a change in ICANN policies or procedures. Indeed, before any change is contemplated, it must be submitted to the ICANN Board for adoption, and before the Board takes any action, other ICANN constituencies, including governments through the Government Advisory Committee, will have an opportunity to express their views into the process.

Just last month in Marrakech, Morocco, at the ICANN Board meeting, the U.S. Government submitted a formal statement into the Government Advisory Committee expressing our concerns. I have included that statement for the committee's record.

Our concern is as it is now a technical definition, it would hinder continued access to that database for a range of legitimate, critical Government uses, including law enforcement, protection of intellectual property rights, and consumer protection.

I think it is important to note that this statement that we submitted reflects not just the views of the Commerce Department but

the views of the Justice Department, the views of the State Department, Homeland Security, the Federal Trade Commission, the FBI, the IRS, and the Patent and Trademark Office.

In developing this position with the U.S. Government, we have also undertaken considerable outreach to other constituencies, including the financial services sector.

We facilitated a meeting between U.S. agencies and the companies associated with the Financial Services Roundtable, to discuss their concerns, and we are continuing to work with these and other interested parties to make sure their views are reflected in the ICANN decision making process before any formal changes of policy are considered.

We have also been working closely with other national governments to develop more formal public policy positions, so those views on the purpose and use of WHOIS data can also be reflected.

Finally, I would also note that the ICANN Board passed a resolution in June that acknowledges the open dialogue between the Government Advisory Committee and the GNSO Council, regarding the issues covered by the WHOIS Taskforce, as well as an opportunity for public comment. We think this is a strong development, and will certainly be a continued opportunity, not just for governments but other interested parties to have their views expressed before ICANN makes any decision on a formal change to its policies regarding WHOIS.

Again, I thank you for inviting me. I look forward to any questions you may have.

[The prepared statement of Mr. Kneuer can be found on page 97 of the appendix.]

Chairman BACHUS. Thank you.

Director Harrington?

STATEMENT OF EILEEN HARRINGTON, DEPUTY DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Ms. HARRINGTON. Thank you, Mr. Chairman. Thank you very much. I am pleased to present the Federal Trade Commission's testimony this morning, which has been entered into the record. My statement and any questions that I provide reflect my views and not necessarily those of the full Commission.

As my colleague mentioned, ICANN recently met in Morocco to continue its consideration of a proposal to narrow the purpose of WHOIS databases, and thus limit access to the useful and important information they contain.

Because this is an issue of great importance to law enforcers and consumers, Commissioner Jonathan Leibowitz of the FTC, along with officials from several of our consumer protection and law enforcement allies from other nations, attended the ICANN meeting to speak about the importance of maintaining access to WHOIS databases.

In the wake of the Morocco meeting, we understand that ICANN is re-evaluating its earlier inclination to adopt a narrower purpose.

The debate over access to WHOIS databases raises at least four important considerations. The ability of law enforcers to access information about fraudsters who use Internet Web sites, the ability

of consumers to know who they are dealing with when they engage in e-commerce, the needs of some private sector entities, including financial institutions, to access WHOIS data to serve important public purposes, and individual privacy interests.

In the brief time I have this morning, I want to elaborate on the law enforcement, consumer, and business entity interests in retaining WHOIS access. I know the important privacy concerns will be addressed by members of the second panel this morning.

The FTC makes frequent use of its authority to stop unfair and deceptive acts or practices to challenge a variety of Internet-related threats, including phishing, spam, and spyware.

In these cases, our investigators face the sometimes daunting task of determining the identity of scoundrels who hide behind the electronic shield of the Internet. Sometimes, we unmask the wrongdoers by learning their identities and whereabouts from WHOIS databases, but even when scamsters provide false registration information, access to WHOIS databases provides invaluable leads.

Scammers often provide the same or similar phony information for multiple Web sites involving several different schemes, and by having access even to that inaccurate information, we are able to develop evidence demonstrating critical linkages that ultimately can help lead us to the bad guys.

Consumers also need to know who they are doing business with, whether online or in the bricks and mortar world, and continued public access to WHOIS data provides the information that can be essential to consumer confidence in the online marketplace.

If consumers do not receive the goods or services that they have purchased, they need to know how to reach the vendor that they have done business with. We really cannot afford to take away the consumer confidence in the marketplace that access to that information provides.

We know that phishing and identity theft are of particular concern to the committee, and they are to the FTC as well.

Financial institutions are watchdogs, private enforcers, and sometimes victims of phishing schemes. They receive early warning from their customers who have received bogus e-mails from phishers, and they can warn their customers. They can sometimes bring private actions to halt the misappropriation of their good names and reputations, and when their customers fall victims to phishers, their reputations suffer.

They, too, are among the private sector entities who need continued access to WHOIS registration information for commercial Web sites. Without it, the risks of identity theft add harm to consumers and can only grow.

WHOIS databases are one source of valuable information for the FTC's work to protect U.S. consumers. There are other critically important tools that the FTC needs, however, to fight online fraud in the global marketplace.

The FTC has previously recommended that Congress consider enacting the U.S. Safe Web Act, which passed the Senate in March of 2006. This act would make it easier for the FTC to gather information about Internet fraud from sources other than WHOIS databases, including our foreign law enforcement counterparts and financial institutions in the United States, and critically, we would

be able to obtain information from financial institutions without tipping off the targets of our investigation to the existence of the ongoing law enforcement inquiry.

We thank you for your attention to the FTC's interests this morning and look forward to answering any questions that you may have.

[The prepared statement of Ms. Harrington can be found on page 82 of the appendix.]

Chairman BACHUS. Thank you. Mr. Hensarling, do you have any questions at this time? If you would like a few minutes, I could go ahead.

Mr. HENSARLING. I am happy to go now, Mr. Chairman.

Chairman BACHUS. Okay. Thank you.

Mr. HENSARLING. As often is the issue in the financial concerns of this committee, there is always a balance between our privacy and our security. I think this issue is re-presenting itself here today.

Mr. Kneuer, if the more narrow definition of the purpose of the WHOIS database was adopted, what precisely is going to change for law enforcement? How does their job become more difficult?

Mr. KNEUER. I think it immediately becomes much more difficult, as Ms. Harrington was just mentioning, when there is evidence of malfeasance on an Internet site, whether it is financial fraud or child pornography or other forms of obscenity, whether it be the abuse and violation of intellectual property rights, the holders of those property rights and law enforcement can go to the site and find out the information.

If the information is unavailable, the Internet potentially becomes an immediate safe harbor for a host of illegal activity that can be accomplished over the Internet without any recourse for law enforcement to really be able to track down the bad actors in an efficient way.

Mr. HENSARLING. Ms. Harrington, essentially the same question for you. How would the FTC be limited by this more narrow definition?

Ms. HARRINGTON. I agree with what my colleague just said. Specifically, there are hundreds of consumer protection and law enforcement investigations going on at any time at the FTC, investigations that often are spurred directly by complaints from citizens and consumers about harm that they have experienced.

The immediate impact is to make it far more difficult for us to find the wrongdoers, and if we cannot find them, we cannot stop them. Most importantly, we cannot get money back for consumers who have been defrauded.

Mr. HENSARLING. If I heard your testimony correctly, you said something that struck me as a little bit curious, and I think I heard you say that even inaccurate information gained from the database can be useful by law enforcement.

If I heard you correctly, could you elaborate on that?

Ms. HARRINGTON. Let me give you a good example. In a case that we brought several years ago in 2002 against a fellow named John Zucarinni; he had registered approximately 6,000 domain names and most of those mimicked legitimate and popular Web sites.

When consumers mistakenly entered onto his turf, their computers were hijacked, their browsers were hijacked, and they really lost control of their computers. It was a horrible situation that he caused.

In that case, we used WHOIS to identify different domain names that were registered to him under different alias, and that inquiry enabled us to assess the extent—what turned out to be the very wide extent—of his bad acts. That was critical evidence in enabling us to go into Federal Court, get an order to immediately shut down all of his Web sites, and ultimately get a judgment for $1.8 million to redress consumers, and then we worked closely with criminal authorities who convicted him of criminal acts, and he served 30 months in prison.

That evidence from WHOIS, even though it was inaccurate, was critical. It told us that we weren't dealing with some small potato operator, but this was a very large scam, and that evidence, in turn, was furnished to criminal authorities when we were finished with our civil case, and that helped them get a significant sentence against him.

Mr. HENSARLING. You also mentioned in your testimony the U.S. Safe Web Act.

Ms. HARRINGTON. Yes.

Mr. HENSARLING. On the other side of the Capitol, one of many pieces of legislation written by the other body that I have not gotten around to reading yet.

Could you elaborate somewhat on, I suppose, the tools that you feel the FTC is missing today to effectively combat this type of fraud, and what are the tools that are provided to you under this act that you desire?

Ms. HARRINGTON. There are several basic abilities that it would give us to obtain and share information with our foreign counterparts. Right now, we cannot.

In addition, a really important provision in U.S. Safe Web would enable us to go to court to get an order to shield—to protect information about a subpoena that we send to a financial institution so that the financial institution would not be required under other privacy acts to notify accountholders that they had received a subpoena from the Federal Trade Commission for information.

Right now, very important investigations, the existence of them, can be revealed and sometimes is revealed by financial institutions to the targets. The effect that has is that when we seek in an ex parte proceeding an asset freeze on the assets of companies that are defrauding consumers, the assets are gone by the time we get there.

It is really important.

Mr. HENSARLING. I see my time has expired. Thank you.

Chairman BACHUS. I thank the gentleman. Mr. Moore?

Mr. MOORE OF KANSAS. Mr. Chairman, I do not have any questions. Thank you.

Chairman BACHUS. Mrs. Maloney?

Mrs. MALONEY. I just want to say that 19 States, including my home State of New York, have responded to identity theft by enacting laws that allow individuals to restrict access to their credit reports whenever they feel it is necessary to prevent identity theft.

Would that not help break down or stop what you are saying is the number one or the highest form, that identity theft comes ahead of any other consumer fraud complaint, accounting for somewhere between a third and a half of all complaints filed with the FTC?

Would not this approach of just allowing file freeze by consumers on their credit—if they want someone to see their credit, then they can release it. It just seems that is the way to crack down on identity theft, which is really an incredible crime.

We have many cases come to my office. Sometimes they think they even make up the numbers, but by the time they find out about it, their credit is ruined really for the rest of their life. They cannot really get it replaced. It is just a very difficult thing.

I guess my question to you is what about file freeze? Would not file freeze work? It stops the thieves from getting the new credit?

Ms. HARRINGTON. We are right with you on the seriousness of the identity theft problem. Consumers now can put fraud alerts on their credit reports, which are a pretty effective hurdle to the issuance of new accounts in their names, and also give consumers pretty much real time information about who is making inquiries, and what is happening with their credit record.

The freeze issue is an interesting one. I think we can argue certainly the pros, as you have very eloquently. One of the concerns with freezes, and when consumers ask us whether they ought to put a freeze on their account, we need to tell them also that what this means is they are not going to be able to access credit in the ways they often want to.

I think it is a balancing act, really.

Mrs. MALONEY. Any other comments?

Mr. KNEUER. Just to stress the importance of WHOIS data for law enforcement; it goes beyond just consumer protection. It is critical for law enforcement in a host of areas.

The FBI feels strongly enough about this that they send representatives to ICANN meetings around the world to ensure that WHOIS data is protected.

Mrs. MALONEY. In late June, in Morocco, ICANN specifically stated that they would continue to provide access to law enforcement in adopting the new rules. Are you aware of this position?

Mr. KNEUER. I think that reflects the view of the Board of ICANN that the views expressed by the GNSO Council were the views of one ICANN constituency, and that law enforcement remains a very important constituency as well, and that before they make any decision on a change in WHOIS policy, the views of law enforcement will be considered.

Mrs. MALONEY. At this forum, they said they would provide access to law enforcement. If law enforcement has access, does that affect your views? It seems that solves it if law enforcement has access.

Mr. KNEUER. I would have to see the full text of the statement, but I believe that is a reflection of the fact that the current WHOIS policy and the current WHOIS procedures of ICANN have not changed.

Law enforcement gets access through the publicly available searchable accurate WHOIS database. They do not intend to make

changes that would adversely affect the ability of law enforcement to continue to have access.

Mrs. MALONEY. I think we all agree that law enforcement should have access. I think we can also agree that the widespread availability of personal information is clearly contributing to the problem of identity theft, which the FTC has reported as the top consumer complaint.

Have you undertaken any studies to determine whether unrestricted access to WHOIS data might not actually contribute to the problem of identity theft and online fraud?

Has the FTC looked at whether spammers are obtaining e-mail addresses and other contact information from the WHOIS database?

Ms. HARRINGTON. We are very concerned about protecting the privacy of individuals' personal information. That is why we have called for public access to registration information about commercial databases, not non-commercial databases. We strongly support continued public access to commercial information.

We did a study. In Internet time, it is probably ancient at this point. It was done a couple of years ago. At that time, it did not appear to us that there was significant use being made by spammers of WHOIS data.

More recently, I have read other more current work that has been done that suggests that may be becoming a problem, and it is something that I think we will be looking at again to update our older work.

Mrs. MALONEY. Have you contacted your colleagues overseas that are operating under privacy rules? Have you spoken with your colleagues in other countries about how the FTC could investigate fraud and still safeguard privacy?

Ms. HARRINGTON. Yes. People from the FTC are in very regular contact with our colleagues in other countries. As the private interests and laws pertain to WHOIS, it is our understanding that, for example, the position that we are taking on continued access to WHOIS registration information for commercial Web sites for the public is not inconsistent with those privacy laws.

Chairman BACHUS. Thank you. Mr. Pearce?

Mr. PEARCE. Thank you, Mr. Chairman. I suspect I would ask either one of you, how big a problem is the identity theft coming from the other side? I tend to fall on the side that if someone is seeking access to me to do business, that I ought to be able to have full access to information to them.

What drives the concern on the other side? Is it based on fact or is it just the concern that we are going to give away information about Web site operators?

I will let both of you take a stab at that.

Chairman BACHUS. Could I ask the gentleman to yield?

Mr. PEARCE. Sure.

Chairman BACHUS. I will ask unanimous consent to give him an extra minute.

I think what Mr. Pearce has just said, I would like to associate myself with his remarks. What he said is if someone has assumed an identity and is contacting me over the Internet and telling me

they are my financial institution or American Express or the Red Cross.

We have a letter from the Red Cross that after Katrina, millions of people were contacted, and after the tsunami, millions of people were contacted, and told it was the Red Cross, and were given a Web site address to send contributions.

As far as privacy, I think the privacy arguments are where Mr. Pearce says, with the consumer, who the identity of the person he is dealing with, he is being told it is his bank.

I will say this. Even the FTC, which says we are going to give law enforcement these rights, but we are not going to give them to individuals, it is the individuals who are being contacted and ripped off.

When you deny the individuals the right to know who they are dealing with and who is coming into their computer and communicating with them and corresponding with them, I think you take away a right that we have had on the Internet since this database started.

They are now saying they want to make changes. It is a radical change that I do not think the American people realize.

A bank robber could claim that taking his fingerprints is an invasion of privacy. I would equate these people who masquerade as my bank or as the Red Cross are criminals. Protecting their identity is sort of like protecting a bank robber's identity.

Ms. HARRINGTON. Mr. Chairman, if I could just clarify. The Federal Trade Commission supports full access by law enforcement to all WHOIS database registration, including—

Mr. PEARCE. That is not my question. My question is for me as a consumer.

Chairman BACHUS. Right. I think in his question, that is maybe what you missed. He is saying as far as privacy and as far as somebody communicating with me, if they are coming on and telling me they are somebody and I am opening up my database and I am giving them information, not only law enforcement, but this is an important tool that consumers have had.

I hope that the FTC, in trying to compromise with WHOIS and ICANN, does not give away important rights of consumers.

What Mr. Pearce is saying, when he deals with somebody over the Internet, they are asking him for sensitive information, and representing themselves as his bank or something.

The fact that the FBI or the local police have a right to that information—

Ms. HARRINGTON. We agree. All of those examples that you have given would fall in the category of commercial Web sites. If someone is posing as your bank, someone is trying to collect money from you, that is information that we believe that you as a consumer, registration information, should have access to.

We draw a distinction between commercial and non-commercial Web sites. On the non-commercial side, some have suggested a tiered access system. There is a lot of debate going on at ICANN about that.

The concern is that if you as an individual have set up your own personal Web site for some non-commercial purpose, if you are a dissident living in some totalitarian regime and have put informa-

tion on the Web site that could subject you to very serious consequences, should your personal information be widely searchable in a WHOIS database by anyone or not?

That is where the personal—

Mr. PEARCE. That was my question. What is the whole question of personal privacy? If my granddaughter is on a Web site that begins to explore pieces of conversation with her that I would rather not have occur, that is not a commercial transaction, and yet I think, for myself, I would sit here in full transparency, there ought to be a click on every communication that allows you to go straight to and find out who it is that really is operating.

I am wondering what drives the debate? You are talking, Ms. Harrington, about the debate being driven by privacy concerns.

You are out here in a full operation requesting information from somebody, commercial or non-commercial, and I just believe that transparency is the better rule. Let's open it all up. Let's shine the light in there. I do not think there ought to be protections of any kind if you are out on the Web trying to get access to my house, my business, or my granddaughter.

I do not understand that. Could you help me understand the legal concerns of privacy?

Mr. KNEUER. If I might, sir. The U.S. Government's submission to the Government Advisory Committee of ICANN makes no distinction between commercial and non-commercial addresses.

It is the view of the U.S. Government, like I said, the views of the State Department, the Justice Department, Homeland Security, the Commerce Department, the Patent and Trademark Office, the IRS, and the FBI, that there should be no distinction between the two of these, and for precisely the reasons you are talking about.

I think Ms. Harrington's views from a commercial standpoint, the equities that the FTC is concerned with, is consumer protection in commercial situations. There are other significant Government equities that have broader concerns, the ones you mentioned.

If a Web site is up that is not necessarily doing commercial transactions, it can be violating laws in a variety of different ways. It could be abusing intellectual property rights. There could be child pornography or other obscenity, where there is recourse to the laws.

We do not make that distinction. We believe that the WHOIS database ought to be publicly available, accurate and searchable for all domain registrations.

Mr. PEARCE. Ms. Harrington, do you have any other ideas or comments on that? What would you say to a link on every communication on a Web site that takes you right to that?

Ms. HARRINGTON. To the registration?

Mr. PEARCE. To the Web site, let you know who it is that has set this particular site up.

My wife serves on a bank board. Just recently people were intercepting communications intended for the bank, representing themselves as the bank. Actually, transactions were occurring.

If that e-mail had access to whoever is originating, the consumer could click on it, take a look and say that is not my bank, this is somebody in Indonesia or somewhere.

Ms. HARRINGTON. I have not thought about that particular mechanism, Congressman. You raise indirectly another really interesting challenge in this whole area, and that is accuracy, which is something that the U.S. Government, including the Federal Trade Commission, has consistently raised as a concern in connection with WHOIS databases.

We want to make sure that there is access to the registration information. We also want to make sure domain registrars do everything they can to ensure the accuracy of that information.

Our experience is oftentimes people who are up to no good include in their no-good activity the providing of false information.

Mr. PEARCE. Thank you, Mr. Chairman.

Chairman BACHUS. Thank you. I appreciate your remarks.

Congresswoman Kelly has been very active on this issue. I have been going back and forth. Mr. Moore?

Ms. KELLY. Are you in the first or second round of questions?

Chairman BACHUS. Actually, he did not ask questions. Go ahead, Ms. Kelly. You have been a leader on this issue.

Ms. KELLY. It certainly is the floor for Mr. Moore.

Chairman BACHUS. He is fine.

Ms. KELLY. Thank you. I think the public's concern on a lot of this is the fact that on Web sites, when you log on to certain Web sites, there are things there that are down right errors. There is misrepresentation.

Apparently, you are supposed to look at who has what Web site, if I understand. Is that correct?

Once you do that informational piece to find out who has established a Web site, do you have any further duty to make sure that what is on that Web site is accurate?

Mr. KNEUER. On the WHOIS database, to test the accuracy of that?

Ms. KELLY. Right.

Mr. KNEUER. The registrars are supposed to ensure the accuracy of it. Given the millions and millions of Web sites, I think it is one of the reasons it is important that it not just be law enforcement but consumers who have access, this really is a collaborative effort, whether it be law enforcement or a consumer who does the initial inquiry, if they see information that appears to be inaccurate or based on that information, they do a follow up and find it leads to a dead end, they can then report that problem, and the registrars can correct the problem or eliminate the Web page.

Ms. KELLY. How would a broad consumer use change that?

Mr. KNEUER. I think broad consumer use is what helps that process along. I think eliminating that broad consumer use makes it much more difficult for the registrars and others to maintain the accuracy of the database.

There are limited resources for the ability to spot check and go through millions and millions of sites.

Having the opportunity for consumers and for others to exercise their rights to get into the WHOIS database to follow up on that information is much more likely to uncover inaccuracies and uncover illegal or otherwise inappropriate activity.

Ms. KELLY. Getting into that database, if I were a consumer, could I change information on the database at my will?

Mr. KNEUER. No. Only the registrant can change the information by submitting it to the registrars, and the registrars maintain the database.

If you go to one of the registrars and clock on WHOIS and you put in a field, I want to know who owns what site, that pulls up—you do not then have rights to edit that field. It is a read-only file.

Ms. KELLY. Do you think that there is an adequate—that we have maximum data and you have so many different Web sites, what do you think is the best thing that you can do to make sure you get the maximum data security and consumer protection without harming the people who are likely to be using those sites, especially small businesses? That is one of my chief worries here. They do use the Web sites.

Mr. KNEUER. I think transparency and consumer education. When I talk about consumers, I am not just talking about individual consumers, but businesses as consumers. As long as there is transparency in the process, more people are aware they have this tool at their disposal.

If you are a small business and you are engaging in business online, you are trying to use the power of the Internet to leverage your small business nationally or even globally and in doing that, you are looking to find business partners, the more ability for those small businesses to access the WHOIS data to find out more about the potential partners that they may be looking at, too, I think the better for it.

To the extent that the WHOIS data, as I said, is itself transparent, when you register a domain name, it is very clear that part of the deal is you are going to publish this information to the world. If you want to publish your Web site to the world, you are going to publish this information to the world.

It is a deal that you make, and it is transparent. This information is not being publicized without the registrant's understanding that it is being publicized.

Ms. KELLY. I'm going back to what I asked before. If the registrar registers the site, does the registrar ever go back and check to make sure that site has not been altered and changed in some way?

The reason I am asking this is I logged onto a Web site which then automatically put me into a second Web site. This was a Web site that is used by private detectives and people like that. People can also get on the site, but when you pay through the second site to get more information, but logging onto the registered site took me immediately to a second site. That second site, when I was happy to pay, because I wanted to see what was on it, had misinformation.

That is what concerns me. The transparency is great. Unchecked transparency can possibly lead to abuse. I am wondering if there is any kind of a screen there that can stop that.

Mr. KNEUER. As far as the ability of a registrant to submit their WHOIS data and then to change it after the fact, I would have to get back to you. I believe those updates are made by the registrars, that you have to submit that to the registrar and have them make the change.

I will get back to you for the record on whether or not I am correct in my understanding of the way that operates.

As far as successive sites, when you get into a site that sort of scrolls down to other sites, you should still have the actual address of the site, even when you default into and you are redirected, the address should be there, should be visible and transparent to you, and then you can do a WHOIS search on that again.

I certainly concede that is sort of the kind of thing that presents a challenge, not just to consumers, but even sophisticated users. It is not real clear sometimes unless you are really ever vigilant.

I concede that is a problem.

Ms. KELLY. Thank you.

Chairman BACHUS. Thank you. Let me first say, Mr. Kneuer, I would like to associate myself with your remarks in the dialogue. I think both of you recognized that there is a real key role for the consumers here.

It is a role they are playing today. The status quo today is transparency. What this proposal would do is take rights away from consumers, everyone that uses the Internet.

There are many legitimate rights that consumers have now, essential rights, to protect themselves, that if this proposal in my mind goes through, then yes, the commercial firms, your bank, they may have rights, and law enforcement may have rights, but the first line of defense, and Mr. Kneuer, you said this, the first line of defense ought to be the consumer.

We say the consumers are responsible for protecting their own information. If we deny them a right that they have presently, this right to know the domain name and the identity, then we are denying them the ability to protect themselves.

There are other things in your testimony that you talked about, Ms. Harrington. I was trying to find it here. You talk about how consumers now have the ability to resolve problems with online merchants directly through the use of WHOIS databases.

They find out who it is and they resolve their problem. Government does not have to deal with it.

You are talking about consumers and legitimate businesses, that if this changes, they are going to come to you and say we do not know who these people are, we have a complaint, you need to find out who they are. You are going to throw a whole lot more work on the Government and individuals, which they are doing now.

You would throw a whole lot more work—I would just like you all to respond to that. I think you put the burden on the Government and law enforcement, the banks and the financial institutions, that consumers could legitimately say if this goes through, I no longer have the ability to resolve this myself.

Ms. HARRINGTON. Mr. Chairman, I think that is right, although I would hasten to add that we are here to serve consumers. We welcome their complaints. We hope they do not have problems, but when they do, we are in the business of serving them.

I think an equal problem here is that consumers will lose confidence in this marketplace if they do not know who they are dealing with. I think that would have very serious implications.

Chairman BACHUS. In fact, we had talked about that on many occasions. Our policy, if they lose—when we talk about identity

theft, we said it is very important for us and the FTC and law enforcement to act against identity theft because it diminishes the use of the Internet. It diminishes people's confidence in the Internet.

To me, the more I look at this, the more I see it as a serious threat to confidence on the Internet, to know who you are dealing with.

Mr. Kneuer, what is the relationship between the Department of Commerce and ICANN? It is my understanding within the ICANN organization, there is a weighted voting by different interested parties.

Could you describe how that works and how it impacts the process? Does that weighted voting bias the process toward certain views?

Mr. KNEUER. The relationship between the Department and ICANN is memorialized in this Memorandum of Understanding.

ICANN is the private sector entity that was established to take over the management of the domain name system. It used to be a U.S. Government function, and a long history of the Internet going back to DARPA and its development as an U.S. Government network.

The MOU is intended as a transitional document for us to provide some oversight over ICANN as they get themselves stood up and become a sustainable secure organization.

As far as the weighted voting goes, that is not in the decisionmaking of ICANN itself. These are not final decisions of the Board of ICANN. These are in some of the subgroups of ICANN, the GNSO being one of them.

When the GNSO was established, they determined that weighted voting to reflect different constituencies in that subset would be appropriate, so there is weighted voting in that Council, in that organization.

That does not carry over into the final decisionmaking of ICANN. The Board of ICANN is elected and representative, and there are not weighted votes in final decisions of ICANN. It is in this subconstituency, this GNSO Council.

Chairman BACHUS. You mentioned GNSO. That states that the, "Current definition of WHOIS data is related to the service that provides public access to some or all of the data that is collected, and is not a definition of the purpose of the data itself."

That seems to me like a definition that believes the WHOIS database service, that their only purpose is maintaining the Web site, which there is another purpose, legitimate purpose; is there not?

Mr. KNEUER. Absolutely. ICANN by its definition, by its by-laws, is supposed to be a consensus driven organization that takes lots of different views. That is one view of the GNSO.

It is clear the governments feel that there are different uses and different purposes for the WHOIS data. Consumers may feel very differently.

The reason ICANN is organized the way it is, is so there is the ability to get the views of all of these different constituencies and all these different equities are represented and weighed going into it.

While one subgroup may have one view, that is not reflective of the overall Internet community as a whole, and it certainly does not reflect the U.S. Government's position or the views of many other governments, as have been reflected in the Government Advisory Committee meetings.

I think you will see much more of that, of the view that the purpose of the data should not be decided by any one group. The important thing is that the data is available, and you can make what use of it that you will.

Chairman BACHUS. I agree. I think ICANN actually ought to consider ways to protect the consumer and ways to protect an individual's privacy.

I will just say this another way. It is almost as if there are all these essential legitimate uses that consumers are taking of the WHOIS data, and it is all of a sudden that ICANN wants to sort of put the genie back in the bottle and stop a lot of these, what we take for granted every day, as our legitimate uses of that data by consumers.

Mr. KNEUER. I think that gets back to not having a narrowed definition of the purpose. For some varieties of malfeasance, whether it is consumer protections, the fraud, we want to make it stop and making it stop may be—you want to recover assets to the extent you can, but making it stop is the important thing. That is not happening anymore.

Other areas of law enforcement have much different concerns, whether it is cyber security and cyber terrorism, or child pornography. You do not want to make it stop. You want to catch those guys.

The more difficult it is for bad actors to hide behind inaccurate WHOIS data, the harder it is for them to continue to commit crimes on the Internet, the easier it is for law enforcement to pursue them.

We need to reflect the broad interests and equities of the community as a whole and not be too focused on one constituency or another constituency.

Chairman BACHUS. I agree. In fact, it is almost, "the public be damned." This is a better way, a more efficient way, to manage the system. If anything, the people who benefit are the people who are committing the crimes.

Mr. KNEUER. Just to be fair as well to ICANN, the proposal from the GNSO has been submitted, but as the ICANN Board stated in Marrakech, and I would refer back to my testimony for the exact quoted language, they do not intend to make any decision to change the current status quo policy without having the opportunity of governments to give their counter view to the GNSO's narrow definition, without having the opportunity for the public to make their comments.

The status quo today still exists. There has been no change in the policies or the procedures, and there will not be any changes until a broad cross section of interested stakeholders have an opportunity to make their views known.

Chairman BACHUS. I have talked to Secretary Gutierrez about this issue. A lot of people think it is just an arcane issue dealing with a technical issue.

In fact, it has very serious implications and consequences for everyone who uses the Internet. It would change the status quo.

Although my words may seem sort of harsh, if consumers are denied some of these rights, the consequences on them are going to be harsher still.

I will close by just asking is the Commerce Department, and is the FTC, committed to watching out for the best interests of consumers, and are they committed to preserving consumers' present rights to the WHOIS data?

Mr. KNEUER. Yes.

Chairman BACHUS. Ms. Harrington?

Ms. HARRINGTON. Absolutely.

Chairman BACHUS. Thank you. I think that is very important. I very much appreciate that.

Does anyone want to ask any other questions of this panel?

Ms. KELLY. Mr. Chairman, I just would ask the Commerce Department to work closely with ICANN, to try to make sure the information is absolutely as accurate as it possibly can be.

Chairman BACHUS. Thank you.

Mr. KNEUER. We will certainly do that.

Chairman BACHUS. That is a good point, Ms. Kelly.

Thank you very much. The first panel is discharged.

Ms. HARRINGTON. Thank you, Mr. Chairman.

Chairman BACHUS. Good morning to our second panel. Our second panel is made up of Ms. Catherine Allen, CEO of BITS/Financial Services Roundtable. We welcome you.

Also, Mr. Mark Bohannon, general counsel and senior vice president, Software and Information Industry Association, SIIA, and Mr. Marc Rotenberg, executive director, Electronic Privacy Information Center, EPIC.

Ms. Allen, we will start with your testimony.

STATEMENT OF CATHERINE ALLEN, CEO, BITS/FINANCIAL SERVICES ROUNDTABLE

Ms. ALLEN. Thank you very much. Good afternoon, Chairman Bachus, and members of the subcommittee.

My name is Catherine Allen, and I am the chief executive officer of BITS, part of the Financial Services Roundtable.

I also want to acknowledge Congressman Pearce from my home State of New Mexico, where there are a few of us around.

I am pleased to appear before you today on behalf of BITS, the Financial Services Roundtable, and our member financial institutions, with respect to the topic of a proposed change to the WHOIS database within the ICANN.

Thank you, Chairman Bachus, for meeting with executives from Am South representing BITS earlier this year on this issue and taking such an avid interest in it.

BITS is a non-profit industry consortium of 100 of the largest financial institutions in the United States. We are the non-lobbying division of the Financial Services Roundtable, and work as a strategic brain trust to provide intellectual capital and address emerging issues around operations and technology for the industry.

Working groups share successful strategies and best practices for managing risks, reducing fraud, managing IT service provider rela-

tionships, and managing risks in the changing payments' environment, and work with the heads of security, heads of fraud, and heads of payment in these organizations.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with the Government and law enforcement agencies.

With the growth of the Internet and its fundamental role as the foundation of electronic commerce, including financial services, the role of ICANN and its significance has grown exponentially.

It is therefore with great concern that our member institutions have become aware of the proposed change in the type of information to be collected and maintained in the ICANN WHOIS database.

The WHOIS database, just as a background, is very important in that it has three types of information, and all three of these types of information are used when we work with law enforcement to track down fraud.

The registrant contract, which includes those registered for domain names, IP addresses, who owns the name, who paid for the name, and the owner's name and address. Secondly, the administrative contact who you call for billing information. Again, their name, phone number, address, and the technical contact who may or may not be associated with that Web site, who specifies if there is a problem with the Web site and does the technical attributes.

As part of their efforts to combat fraud, financial institutions are constantly watching for incidences of domain name fraud. Sometimes we call it cyber squatting or typo squatting. These are people that will create and register domain names that are very similar to financial institutions, but they might have one slight change to them. In some cases, a changed vowel or a changed name. In any sense, they look very familiar to the consumer and they think they are talking to an actual legitimate financial services company.

In one case, one of our financial institutions found a Web site with a name that was identical to their own, except for the one vowel change. Going to the home page, they saw that it was not only an example of theft of intellectual property, but of course, they were trying to commit fraud against consumers.

Using the registrant information from WHOIS, the financial institution in this instance was able to contact the Web site owner and send a cease and desist letter to have the site removed.

One of the other key uses for the WHOIS database is for shutting down phishing sites. As part of investigating phishing incidences, financial institutions sometimes discover that a legitimate Web site has been taken over by phishers, without the Web site owner's knowledge.

With cooperation of the WHOIS technical contact and the registrant's contact, and the hosting site, they were able to shut down a phishing site. Again, they needed at least two of the three kinds of information.

In early 2006, a financial institution discovered it was being phished from a site in Taiwan. Efforts to have the Web site shut down using the technical contact information was unsuccessful. In

fact, it took the full WHOIS information provided to the U.S. Secret Service and the Taiwanese police, who made local contact with the Web site owner and the ISP and got the phishing site shut down.

These are just a few examples of the reasons that financial institutions and others who are combating fraud find the WHOIS database so important as a tool for fighting fraud and protecting the public.

All of the WHOIS information is currently freely available to anyone with Internet access, and while it may be prudent in some cases to restrict some access, we do believe it needs to have what we call permissible access by all players—law enforcement, businesses, or people who have legitimate reason to try to track down for fraudulent reasons who owns this database.

It is a matter of public confidence. We agree with the discussion that happened with the previous panel, that the more transparency there is, the better it is for all of us, including consumer access to this information.

As you are aware, on January 18th, the ICANN WHOIS Task Force report contained two opposing formulations for the purpose of WHOIS. Under formulation one, which is severely restrictive and just a technical issues' configuration, we believe adoption of that would make it more difficult and time consuming for financial institutions to identify and stop domain based scams and identity theft and account fraud. It will also hinder our ability to respond to identity theft and phishing. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers.

In most instances, many unsuspecting consumers are contacted by a financial institution to learn that they may have been a victim of identity theft and they may not have known it because a Web site had been set up in their name, which turns out to be a fraudulent Web site.

Giving the consumers the opportunity to remedy the effects of the identity theft sooner rather than later is critical, not only to law enforcement, to the financial institution, but most importantly, to the consumer.

Most innocent victims have been, and continue to be, extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is the target or potential target of a phishing attack.

Financial institutions need the WHOIS information to address all of the forms of fraud noted above.

For these reasons, we have urged ICANN to adopt formulation two. Formulation two would provide financial institutions, law enforcement and others open access, continued open access, to the information they need to respond to identity theft and account fraud.

It is our understanding that during the ICANN meetings in Marrakech, the decision to choose between formulations one and two was postponed for additional deliberation.

On behalf of BITS and our financial industry, recognizing that the ICANN Board has the ultimate decision, we encourage Congress to strongly support the adoption of formulation two. Thank you for the opportunity to testify before you, and I will be happy to answer any questions.

[The prepared statement of Ms. Allen can be found on page 46 of the appendix.]

Chairman BACHUS. Thank you, Ms. Allen.

Mr. Bohannon?

STATEMENT OF MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION

Mr. BOHANNON. Mr. Chairman, members of the committee, I appreciate the opportunity to appear before you today and testify on ICANN and the WHOIS database. I particularly want to thank you, Mr. Chairman, for your opening statement, which was very strong and very clear about the importance of this issue, and we want to continue to work with you and the committee to pursue the right policy here.

My organization has been engaged in the issue of WHOIS policy for many years, primarily through our involvement in the Coalition for Online Accountability, which includes most of the major organizations and members of the copyright community.

We see firsthand how the WHOIS database is a key tool to combat copyright and trademark infringement, cyber squatting, fight phishing attacks, as well as combat the pernicious effects of spyware and illegal downloads.

In my prepared remarks, I document how I believe all Internet users, consumers, as well as leading groups such as TRUSTe and the Center for Democracy and Technology, who are committed to promoting privacy network security, depend on the WHOIS database, and I would ask that it be submitted for the record.

I really want to focus on two issues in my verbal comments. One is I want to talk about why the proposed policy is misguided, and secondly, why we have to ramp up and step up efforts to make WHOIS reliable and accessible.

When SIIA and other members of the intellectual property community heard about the move to restrict access in the purposes of WHOIS data, we were obviously greatly concerned.

The formulation that was put forward, so-called formulation one, it is important to understand that it represents only a very, very small proportion of the current critical public interest uses of WHOIS data.

In fact, virtually all the ways that WHOIS is now used to protect intellectual property rights, investigate cyber crimes, fight fraud and phishing and protect privacy online would in our view fall outside the scope of this definition.

When the discussion became more broad, it was becoming quite apparent that the change would be devastating to businesses, consumers, and everyone who uses the Internet in a positive way.

It galvanized many concerns about ICANN's stewardship of the WHOIS system. At the early stage, more than 50 organizations, coalitions, entities, and individuals from over 12 different countries filed comments with ICANN arguing against the narrow formulation of the purpose of WHOIS, and as I believe you, Mr. Chairman, pointed out, even the American Red Cross pointed out that it would have definitely have restricted their ability to go after the fraudu-

lent Web sites that were trying to take money from citizens all in the name of helping those who were victims of Hurricane Katrina.

After the Council vote in April, I would say an even more remarkable broader sector of business and other interests became quite concerned.

I would like to submit for the record letters from diverse sectors, such as financial services, and hotel/lodging, as well as intellectual property and anti-counterfeiting groups.

Chairman BACHUS. Without objection, that will be allowed.

Mr. BOHANNON. Finally, Mr. Chairman, I wanted to directly acknowledge and thank you for your leadership. Your letter to Secretary Gutierrez earlier this year provided very important impetus and urgency to the development of a strong U.S. Government position going into the ICANN meeting in Marrakech. We want to thank you for that.

We also want to take the opportunity to acknowledge the position that was presented by the U.S. Government delegation at the ICANN meeting. Fortunately, their view was reinforced by other governments that were in attendance, including the consumer protection authority in The Netherlands, as well as the representative from the Japanese Ministry of Information and Communications.

While most of our discussion has really focused on public access and why that is critical, we also want to make it clear that it is essential, absolutely essential, to dramatically improve the accuracy and reliability of WHOIS data.

The situation and the problem has been very well documented. In a study released by the Government Accountability Office last December, they estimated that the WHOIS data on over 5 million domain names in .com, .net, and .org, is either obviously false, incomplete, or simply could not be found.

This high level of inaccuracy, in our view, significantly undermines the purpose, the role, and the value of WHOIS to consumers, to businesses, and to law enforcement.

The GAO study also clearly shows that the system that ICANN put in place to address the problem simply is not working. GAO investigators submitted complaints about blatantly false data to the system, but after more than a month, the contact information had been corrected in only one quarter of the cases. At least half of the time, the phony data remained unchanged and the domain name remained as active and accessible as before the complaint was made.

This hearing comes at a critical juncture in the relationship, in our view, between the U.S. Government and ICANN. As you know and as we discussed, the MOU between them ends on September 30th.

When the Memorandum was renewed 3 years ago, ICANN pledged to take steps to improve the accuracy of WHOIS data. It also promised to put in place an enhanced system for ensuring domain name registrars and registries live up to their contractual obligations. That is making the WHOIS data publicly accessible and dealing directly with complaints about inaccurate data.

We understand that ICANN believes that it has fulfilled these pledges under the MOU. Candidly, we do not agree with this assessment. While we believe ICANN has taken some steps to im-

prove the system for receiving and processing complaints, ICANN's own reports show that the system does not work as it was designed to do.

ICANN has consistently shied away from taking on the more difficult challenge of requiring registrars and registries to take proactive steps, any steps, in our view, to actually verify the information they are collecting to ensure that it is accurate and reliable.

Mr. Chairman, as we look forward and ahead to working with you on how best to ensure that ICANN does not set off down a path that would lead to a reversal or substantial erosion of the long-standing policy regarding making registrant contact data accessible in real time without charge via the Web and without substantial restrictions on use, we thank you for this hearing.

We think that the policies are in our national interest, in the interest of consumers and businesses worldwide, and in the interest of promoting the healthy growth of the Internet as a safe place to work, to play, and to do business.

[The prepared statement of Mr. Bohannon can be found on page 69 of the appendix.]

Chairman BACHUS. Thank you.

Mr. Rotenberg?

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman. I appreciate the opportunity to testify today. I ask that my complete statement be entered into the record. I will summarize for you the key points.

Chairman BACHUS. Without objection, all of the panelists' full written testimony will be entered into the record.

Mr. ROTENBERG. Thank you, Mr. Chairman.

My organization, the Electronic Privacy Information Center, EPIC, has been involved in the WHOIS debate pretty much since the beginning. I, myself, am also the former chairman of the Public Interests Registry, which manages the .org domain. We developed, in fact, one of the best WHOIS practices, we believe, of any of the domains operating on the Internet.

I am here this morning to present a view on behalf of consumer organizations and non-commercial users of the Internet, which is very much in support of the effort that ICANN is currently making to protect the privacy of Internet users.

I need to be clear about this point. I believe there was some confusion on the first panel as to what the consumer interest is regarding unrestricted and unaccountable access to the WHOIS database.

Under the current ICANN policy for WHOIS, anybody who has a connection to the Internet can go to this database and get the personal contact information of anyone operating a Web site, a political organization, an arts organization, a human rights organization, a group of hobbyists who have set up a Web site possibly in their living room or their basement—any person can get access to that information and use it for any purpose.

That means that under the current ICANN policy, which the other panelists appear to favor, the person who is committed to

fraud and spam and phishing has the exact same right of access as the law enforcement agent or the consumer protection official who is investigating crime.

This is clearly not a sensible approach to protecting the interests of Internet users.

The problem is so serious, in fact, that as the other panelists have noted, identity theft has become the number one consumer complaint in the United States.

What did the Federal Trade Commission urge consumers to do to protect themselves against this crime? They said be very careful about putting your personal information on the Internet, because it is your personal information, your home address, your telephone number, and your e-mail address, that makes it possible for others to commit types of fraud and crime against you.

ICANN, taking into account the growing concern about identity theft, while recognizing that law enforcement will need access to investigate crime, has appropriately decided to revise their policies for access to the WHOIS database.

The chairman of ICANN, Mr. Twomey, and the various interest groups participating in this process, have not objected to law enforcement access. That is not what the debate is about.

The debate is about whether there should be appropriate safeguards to ensure that the millions of individuals who provide information when they register an Internet domain will not find that their personal information is being improperly disclosed to others.

Just to make very clear how serious the link is between the unrestricted access to WHOIS data and the problem of phishing, which I gather to be a central concern of the hearing this morning, the top phishing investigation and prosecution that was pursued in the United Kingdom was against an individual who took advantage of access to e-mail addresses that he could obtain from the WHOIS Directory to commit the type of financial crime that the other witnesses this morning are understandably concerned about.

It is our view that a sensible and effective approach to the use of WHOIS data is one that will allow people who register Internet domain names to protect the privacy of their personal information. It will still be made available to the registrars. We are not saying contact information should not be provided. We do believe it should be provided, but we think the circumstances under which it should be disclosed should be limited to appropriate and legal circumstances.

There is a very simple analogy here, Mr. Chairman, and that is, of course, the driver's license and driver's record information that all of us provide to the State DMV's as a condition of the right to drive a car on a public roadway.

We make this information available to the Government, and the Government needs to make use of that information oftentimes to investigate crime and theft and accidents.

We would not say that the information in the State DMV databases should be widely available to the general public for any purpose it might choose. In fact, the Congress has wisely chosen on several occasions to protect the privacy of just that type of information so that it is not improperly used.

My point is simply this. If we protect the privacy of the information that is collected to register an automobile and it can still be accessed for law enforcement, for appropriate use, should we not similarly protect the privacy of the information that is provided to register a Web site?

It will still be available for appropriate use, but we do not want it widely available to the public. It is contributing to the problem of identity theft.

Thank you.

[The prepared statement of Mr. Rotenberg can be found on page 103 of the appendix.]

Chairman BACHUS. Thank you, Mr. Rotenberg.

My question is simply going to be, Mr. Bohannon, Mr. Rotenberg gave a different view from the first panel or Ms. Allen and you.

Would you respond to his arguments? Are they valid? How do you deal with that?

Mr. BOHANNON. Mr. Chairman, of course, Mr. Rotenberg and I have worked on a number of things together. Sometimes we agree. Sometimes we do not agree. I think on this one, we do not agree on either the nature of the potential problem that he was describing, much less the overall balance that is trying to be struck here.

Let me try to address—if I miss a point, let me know.

Chairman BACHUS. I will give Mr. Rotenberg the right to respond.

Mr. BOHANNON. I think the question no one on this panel is arguing is that there are not real problems to address with regard to identity theft and how we combat that. I think in this Congress we have seen lots of discussion of that across the board.

The question is whether the kind of information regarding the kind of entities that are on the WHOIS database in fact contributes in any way, much less in a meaningful way, to identity theft, fraud, and anything else. With all due respect to Mr. Rotenberg, I do not believe the evidence is there.

In fact, if you look at the kind of registrant technical and administrative data that is on WHOIS, registrants, in fact, their e-mail address are not publicly available. The only thing you have to put as a registrant is your name and postal address. Technical and administrative contacts, that is different.

When you are talking about the actual registrant, we are not talking about the kind of information that would be associated with identity theft and leading to those kinds of things.

Our view is that the overall balance to be struck here is when my member companies get thousands of complaints in an hour that they are getting fraudulent e-mail and being directed to deceptive Web sites. What within minutes or hours can companies do to shut those down and give their customers confidence that they can do business?

At this point, there is no silver bullet. WHOIS becomes an essential step in combating that. If we were to rely only on law enforcement, we believe that it would dramatically hinder our ability to go directly and help our customers when they are being confronted with these kinds of attacks. It simply cannot be done in minutes or hours.

As you know, Mr. Chairman, our organization has a long history of working in a public/private partnership with law enforcement to combat cyber crimes, intellectual property theft. They do great work, but they cannot operate within minutes or hours like our security offices and our customer relationship folks are required to do.

Chairman BACHUS. Thank you. The WHOIS data, are you disputing that it is being used today to protect consumers and to advance confidence in the Internet?

Mr. ROTENBERG. I believe it is being used in both ways, Mr. Chairman. I believe that the WHOIS data can be useful to investigate certain types of activity. I think you have to be a fairly sophisticated user to use the WHOIS data for that purpose, because a person who intends to commit a crime online is usually pretty good at concealing their actual identity, and that includes the information they would provide for the WHOIS database.

Chairman BACHUS. Would you restrict some of the present rights that consumers have?

Mr. ROTENBERG. I am encouraging an approach that ensures—it is the consumers' information, by the way, that is being disclosed. There are two sides to this coin.

Chairman BACHUS. If you operate a Web site and if you communicate with someone and give them that Web site, then they have a right, but if you didn't want them to have that information, you just simply would not communicate with them; is that right? Wouldn't that solve your problem?

Mr. ROTENBERG. That could be.

Chairman BACHUS. You obviously have some motivation for communicating with that consumer.

Mr. ROTENBERG. You may also be a non-commercial entity. As I said, there are many people who register Internet Web sites for non-commercial purposes. There are many human rights organizations, I should point out, that have found that the Internet is the most effective way they have for expressing their political views and trying to bring democratic reform to some of the governments in this world that need reform.

They are concerned that if their personal information were made available to the governments in which they are operating, they would be at serious personal risk.

If I may, Mr. Chairman, because I know other witnesses had asked that certain information be entered into the hearing record, on this particular point with Mr. Bohannon, I would like to ask that an article that my staff found be entered into the hearing record.

This concerns the spammer in the United Kingdom, if I could just read two sentences.

It begins, "Britain's most prolific spammer, currently behind bars and facing a number of charges, has also just been fined 81,000 pounds."

It goes on to say he, "Used Nominet's WHOIS database to send out fraudulent domain name renewal invoices under the name of Domain Registry Services."

He had access to the WHOIS data, which made it possible for him to commit the fraud.

Chairman BACHUS. Is that the only case you are aware of?

Mr. ROTENBERG. I am sure we could find many more, sir. I just thought it was remarkable. He is the most well-known spammer in Great Britain.

Chairman BACHUS. You would agree there are literally thousands, or tens of thousands, of examples of people who have misrepresented their identity to consumers and thereby committed identity theft or entered into fraudulent practices?

Mr. ROTENBERG. Yes, sir. We certainly support those prosecutions. As I said, we have worked with the Federal Trade Commission and encouraged prosecutions of fraud that does jeopardize the interests of consumers.

We do believe that the interests of consumers are also jeopardized when their personal information is made available online.

Chairman BACHUS. Since this WHOIS database was set up, since day one, consumers have had this information that you are now advocating be withheld from them; is that right?

It's a change to the status quo.

Mr. Bohannon and Ms. Allen are basically arguing for the status quo, and as I understand it, you are arguing that the consumers' right to know be limited.

You have given as a legitimate reason the protection of the privacy of the Web site operators.

Am I wrong?

Mr. ROTENBERG. From our perspective, Mr. Chairman, the consumer right here is the ability to control the disclosure of their personal information.

Chairman BACHUS. Are the Web site operators, I would say 90 percent—it is my understanding you are limiting the right of consumers to get that information which they presently have. Am I right?

Mr. ROTENBERG. We would certainly allow access for appropriate purposes, as I mentioned at the beginning. I was chairman of the .org domain. We are the third largest generic top level domain name. There are millions of people who register .org domain addresses. Many of them are for non-commercial purposes.

Chairman BACHUS. Thank you. Mr. Bohannon? I'm sorry. My time has expired. Mrs. Maloney?

Mrs. MALONEY. Thank you. I would like to ask all of the witnesses. I think we all agree that access to the database can be useful, but can also be a tool for identity theft.

Why not segregate the most sensitive information and keep that private so a consumer might still be able to see who contacted them, but might not get the sensitive personal data that could allow them to set up a fake account in their name?

Could you respond to that? In other words, limiting the amount of information. You can get a name but not the address, so you cannot use that sensitive information.

Ms. ALLEN. Maybe I will start by responding. I think when we are talking about access to the WHOIS database, the only sensitive data is their name, address, telephone number, and in the case of the administrative contact, their e-mail, but there is no financial information that is available.

As the financial industry, we are looking to be able to track back who owns a Web site or maybe the genesis of an e-mail that may be used for phishing to go capture that information from a bank or from consumers.

In the WHOIS database, there is no sensitive data other than the name, address, and e-mail of who owns that database.

Mrs. MALONEY. Any other comments?

Mr. BOHANNON. I think it is important to understand that, in fact, the WHOIS database is already carefully balanced to make sure that sensitive information like billing information the registrars get from the registrants, that is clearly not put on the Web sites. I think we need to recognize that is already a limitation.

I will reiterate my point from earlier, which is you will not find the sensitive information of registrants on WHOIS. You will find their name and postal address. What you will find is contact information for either technical or administrative contacts. In that context, the Nominet example, I think, is very useful. It was a very well-publicized case about 2 years ago.

The system worked. The individual was engaging in illegal spam. Illegal because the registrar accreditation agreement that ICANN has in place precludes use of the information for precisely the kinds of activities the gentleman in the Nominet situation was engaging in.

Our view is that ICANN needs to do more to enforce those agreements, to make sure that the limitations on WHOIS data that already exist are meaningful and are not abused.

When we hear the word, "individual," we need to be careful here. What was involved in almost 99.9 percent of those cases were individuals who were not there as consumers, but individuals who were there in a corporate capacity.

Take me, for example. I have my name and e-mail address on our Web site. Is that me as an individual? Yes. It is me in my capacity representing my members. That is, in fact, the kind of information that this gentleman used, and to reiterate, he engaged in violation of existing ICANN policies, and we think ICANN should be doing more to make sure those policies are enforced.

Mr. ROTENBERG. I think what you have outlined is, in fact, a sensible and effective approach that many organizations and experts and Government officials who are participating in this process at ICANN hope will result.

As the other witnesses have indicated, this policy is still under discussion and a number of different approaches have been put forward. I think there has been very good input.

I believe that a sensible solution is one that will restrict access to personal information and still leave some point of contact for accountability and investigations when appropriate.

Mrs. MALONEY. I would like to ask each of you whether you agree there should be different standards for accessing WHOIS depending on whether an Internet registrant is commercial or noncommercial.

Mr. ROTENBERG. I will say on this point that I know the Federal Trade Commission has proposed this distinction. I think there is certainly some support for this.

A business that holds itself out should be accountable and there should be a point of contact for a business, and we wouldn't necessarily have the same expectation for a non-commercial entity on the Internet.

I think as a broad solution to the WHOIS issue, as my testimony suggests, there will need to be a point of contact for all registrants.

One approach may be to allow proxy registrations so that individuals, for example, will have a buffer, if you will, so that it is still possible to reach someone when necessary, but they won't be directly exposed online.

Mr. BOHANNON. I think the discussions that are underway about the subject are very helpful, and we are participating actively in them.

Congresswoman, I think at this stage, there is little that provides comfort that this could be put into place either operationally or from a practical point of view.

I think even the FTC has acknowledged in its statement that until those are resolved, everything should be publicly accessible, and that there needs to be more information gathered.

Let me just say that the question of commercial versus non-commercial is a tricky one. My organization, SIIA, is a 501(c)(6). Technically, we are a non-profit under the tax laws.

Am I therefore a non-commercial entity who should have my information restricted? That makes no sense whatsoever, since we are actively engaging and holding ourselves out to the public, even though we do not pretend to make a profit.

I think you need to be very careful about the language of non-commercial and commercial when in reality, entities, individuals, organizations that are using a publicly available Web site to promote themselves, to engage in education, and to do other things, are holding themselves out to the public.

I think one point that has been missed, if I could just take a second, if an individual wants, for political or other purposes, to be able to communicate in a meaningful way, getting a Web site, in my humble opinion, is probably the last thing you want to do.

There are lots of ways you can do it through blogs and others that are not registered at the top level domain that I think can be doing exactly the kind of things Mr. Rotenberg talked about, but which avoid, I think, some of the points that are being made.

Quite frankly, if I were engaging in political dissidence, the last thing I would want is a Web site. I would want to figure out how to use an appropriate proxy service or something else, and those are all provided under very clear rules under the ICANN.

This notion that Web sites are nothing, I think we need to get pass that in terms of addressing some of the communication issues that have been discussed here.

Mr. ROTENBERG. Could I respond to that?

Mrs. MALONEY. Absolutely.

Mr. ROTENBERG. I am actually really struck by Mr. Bohannon's comment. I find it extraordinary that an association that represents leading technology companies in the United States would discourage political speakers from taking advantage of the Internet and establishing Web sites.

Mr. BOHANNON. I am sorry. That is not what I said. That is incorrect.

Mr. ROTENBERG. I believe that is exactly what you—

Mr. PEARCE. [presiding] Could the gentlemen suspend?

Mrs. MALONEY. Ms. Allen, if you would respond to the commercial and non-commercial.

Ms. ALLEN. I would. We draw no distinction. In fact, we support the Department of Commerce's position, and believe in transparency. A lot of it has to do with going after the bad guys.

BITS just had a conference last week on anti-money laundering. We were looking at the growth of fraud on the Internet and concerns about the bad guys, and the correlation that has with the charities that sometimes are fronts for terrorism groups, and that they are using that as one of the ways that they do funding.

I think it is important that we have transparency and that it could be a not-for-profit or a for-profit or an individual who has a Web site that may be a bad guy, and we want to be able to have access to that.

Mr. PEARCE. The gentlelady's time has expired. I would request unanimous consent to enter into the record a statement by Lynn Goodendorf. She is the vice president for information privacy protection for the Intercontinental Hotels group, and then also a letter from Mr. Fred Becker, Jr., National Association of Federal Credit Unions. Without objection, those will be entered into the record.

Mr. Rotenberg, on page six of your testimony, you declare that governments are trying to crack down on human rights groups by extending identification requirements for Internet users.

I suspect that is something you would object to.

Mr. ROTENBERG. We do, sir. We work with human rights organizations all around the globe. We are particularly concerned about those organizations that are pursuing democratic reform—

Mr. PEARCE. Sir, if I can go ahead and ask you the question. What position did you all take when Google went ahead and decided to cooperate with China?

It is my understanding they were providing information on who searched the word, "democracy," who searched for words.

What did you all publicly do? What did your organization say about that publicly? What was your position?

Mr. ROTENBERG. We took no formal position and we were not asked to appear before the committee that held the hearing on this issue. We did express our opposition to Google's support for the Chinese based search engine, .cn.

The practice impact of that search engine is to restrict access to information on the Internet that the Chinese Government does not want the Chinese people to receive.

We did not support that.

Mr. PEARCE. You took no public position, but you are taking a public position now that would provide consumers with access to information? Am I characterizing that accurately?

Mr. ROTENBERG. Sir, I would be happy—

Mr. PEARCE. I am asking a question. You are taking a public position on restricting access to consumers. Is that your position?

Mr. ROTENBERG. We do not believe we are restricting access to consumers.

Mr. PEARCE. If I could then go to page three of your documentation, you quote from the Public Interest Registry that, "As the Internet and the number of its users has grown, the justification for making WHOIS data publicly available is no longer applicable."

Did you quote something you did not believe?

Mr. ROTENBERG. I do. I very much support that statement.

Mr. PEARCE. My position still stands. It appears that you are supporting restricting access to consumers, but you are not unwilling to speak to Google publicly when they identify people for the government of a fairly repressive regime.

I really want to get my feet underneath me as far as your positions are concerned.

Mr. ROTENBERG. I certainly appreciate the question, and if I can clarify my response, I apologize if I have not been clear.

We were opposed to what Google did with respect to the search.

Mr. PEARCE. You did not take a public position, right?

Mr. ROTENBERG. To the extent that we were asked our views, that is what we said. As to the public availability and the statement from the Public Interest Registry, which we cite in our statement, we think it is an excellent point that was made in support of WHOIS privacy.

Mr. PEARCE. Can I ask you, in that same quote, "As the Internet and the number of its users has grown, the justification for making WHOIS data publicly available is no longer applicable," how does it affect privacy concerns if we affect the privacy of more rather than fewer, the logic of that position is a little bit untenable. It seems like we would be interested in protecting the privacy of even a single individual, yet the quote specifically states now that the number of people is larger, now we have cause for concern and we are going to take a position.

I am not following that logic.

Mr. ROTENBERG. I believe the point that is being made in the statement and is one that is generally understood at the ICANN, is when the data was originally available, it was to technologists for the technical purpose of maintaining the security and stability of the Internet.

What has happened over time because it is more widely accessible to more people, it is creating new privacy risks that did not previously exist.

That is why we have the problem of identity theft and phishing and spam.

What the Public Interest Registry is expressing here is the recognition, which I believe ICANN is agreeing with, that in this environment, the unrestricted access to personal information poses new privacy risks.

Mr. PEARCE. I had asked the previous panel if it were possible if all Web sites had a link straight to the WHOIS database. I suspect you would be opposed to that.

Mr. ROTENBERG. I think it could be helpful for consumers who are dealing with businesses online.

Mr. PEARCE. No, I did not ask about businesses. I said, "all." It goes back to the discussion about my granddaughter, what Web sites might be misleading my granddaughter.

I think there would be a very good reason to have the capability for a parent to go in and check to see who exactly is talking to a daughter in non-commercial means.

You would oppose that?

Mr. ROTENBERG. I would be concerned that the same policy might be applied to a Web site that your granddaughter would choose to create on the Internet. I think she would have a privacy interest in protecting—

Mr. PEARCE. If my granddaughter wants to go on the Internet and begin to represent herself as someone, I think she should be responsible enough to be asked who she is and where she is located. I do not fear that at all. It is part of transparency.

Mr. Baca, it is time for you to ask questions.

Mr. BACA. Thank you very much. Let me ask all three of you just a simple question at the very beginning, and you can just answer it yes or no.

Dealing with identity theft, it seems like individuals now can obtain any kind of information, more information, using the Web sites and the Internet. It has become a serious problem because some people may give out a little bit more information, so therefore, they have access.

Is that true? Just for the record, yes or no?

Mr. ROTENBERG. I would say yes, it is a risk when people make more information available online. It can be misused.

Mr. BOHANNON. I am not sure I understand your question, Congressman.

Mr. BACA. Right now, since we have a lot of identity theft, is there a probability that now more individuals are at risk because they are using the Web sites, they are using the Internet, that they are giving out a lot more information, so therefore, other individuals may have access to that information? Yes or no? Just a simple yes or no.

Mr. BOHANNON. I apologize. The question you are asking is of course, way beyond the scope of this hearing. I am trying to make sure I give you—

Mr. BACA. We are talking about theft, fraud, the Internet.

Mr. BOHANNON. If I make more information available online or offline, yes.

Mr. BACA. Thank you.

Ms. ALLEN. The answer is yes, and right now, more identity theft comes from off line, from dumpster diving, than online.

Mr. BACA. Thank you. The next question is what steps can consumers take to protect themselves against phishing, which is number one? This question is for Mr. Rotenberg.

Is there a one-stop-shop of information that I can refer them to?

Mr. ROTENBERG. The main advice we give to consumers is to know the Web sites that they are dealing with, and to limit the amount of personal information they provide, but when they do run into trouble, we encourage them to visit the Web site of the Federal Trade Commission, the Privacy Rights Clearinghouse, and also the Identity Theft Resource Center, all very good resources for consumers.

Mr. BACA. Thank you.

Mr. BOHANNON. I think Mr. Rotenberg outlined a number of very important steps. The other thing that virtually every company that does business has developed is a means to get from their customers examples.

I, for one, use a very popular online payment service personally. I send to spoof@ that entity so many times a day that I think it helps them keep up with what is going on.

I think it is very important in addition to the examples that Mr. Rotenberg talked about, to be in direct contact with the company that you are doing business with so that they know and they can tell you whether or not it is legitimate or not.

Mr. BACA. Ms. Allen?

Ms. ALLEN. The same thing, consumer education and knowing who you are doing business with.

Mr. BACA. My next question is is there some kind of educational program that we could put out to our consumers right now? All three of you suggested some ideas. The problem is that many of our consumers are not aware there is this information that they could access or go through.

How can they find out information, or is something we should be doing even here at the national level, developing some kind of educational consumer awareness?

Mr. ROTENBERG. I think the Federal Trade Commission has done some good work in this area. I think the businesses are also doing a fairly good job trying to encourage consumers to learn more about doing business online.

Part of the problem, Congressman, is that things are changing very quickly. Technology is changing quickly. Businesses are changing quickly. A year ago, no one had heard of MySpace. Today, it is the number one Web site. It has a big impact on the privacy of our children.

It takes a lot of time and effort to stay up to date with these developments.

Mr. BACA. One other question. A lot of us, under the identity theft and fraud that is going on, a lot of us sit home, it doesn't matter who we are, and get a lot of the telemarketers who call us almost on a daily basis. Now, at least we have developed a block number so we can block some of those out.

Is there a computer type system available where we can actually block some of this out? That is where a lot of the identity theft and fraud also occurs, and I don't know if our consumers are aware if there is some type of a system that is available that can block out, like we do block out numbers. Right now, anybody can get into the Web site, the Internet, e-mail.

Is there such a system that is being developed, and if there is, some of us need to be educated. Maybe I am not aware.

Mr. ROTENBERG. Congressman, as you indicated the Do Not Call legislation was extremely successful. There were more than 100 million consumers who signed up for that. It did reduce the amount of telemarketing and the phone calls at dinner time.

There have been proposals since for a Do Not E-Mail list, but it is not clear those would be effective. Most of the efforts to restrict the amount of spam that consumers receive are working forward on the technology front and not so much on the legislative front.

Mr. BACA. Could you elaborate? Why would it not be effective? You said it may not be effective?

Mr. ROTENBERG. There are many reasons. One of them is that e-mail addresses can be imprecise. They can change. It can be difficult to identify the originator of an e-mail communication. It is also very inexpensive to send millions and millions of e-mails.

It turned out that it worked, the Do Not Call list worked particularly well for telemarketing because of the structure of the industry and the ability with legislation to limit some of the more invasive practices.

Mr. PEARCE. The gentleman's time has expired. Ms. Kelly?

Mr. BACA. Could I have Mr. Bohannon's answer?

Mr. PEARCE. One moment, Ms. Kelly. We have one more answer.

Mr. BOHANNON. Again, Mr. Rotenberg and I often agree on many things, and this is one. I would just refer to the Congressman and the committee a very thoughtful study that was done by the FTC in response to Congress on this very question, where they identified not only many of the practical issues that Mr. Rotenberg identified, but you can imagine a hacker—a hacker would spend every night for a year trying to figure out how to hack this database.

A, he knows or she knows they are legitimate e-mail addresses. If he ever gets ahold of them, he could spam everyone in the world.

I think there are a number of issues that come up with a registry like approach and Do Not Call, but the other point I would add to the very thoughtful comments is I think there are some good tools out there to help you in managing some of this. They are not perfect. Some of them are my members.

I do think it is important to know the tools that are out there, keep them up to date, and know how to use them so you become as sensitized and are as aware of what is trying to get to you, both good and bad.

Mr. BACA. As we do that, we have to simplify it for some of us who are not technology connected. It needs to be very simple.

Mr. BOHANNON. I can tell you some suggestions. I am not allowed, of course, to promote particular products here.

Mr. PEARCE. Thank you. Ms. Kelly?

Ms. KELLY. Thank you very much, Mr. Chairman.

You three were in the room when I was asking a question of ICANN and the Commerce Department. My question to you is do you think the Commerce Department ought to require ICANN to carry out random audits of the register and the WHOIS data procedures?

Let me start down at the other end, Mr. Rotenberg.

Mr. ROTENBERG. Thank you, Congresswoman. I think audits could be helpful, if you were trying to encourage accuracy, but I also think that our privacy safeguards would encourage accuracy.

One of the reasons that people provide inaccurate information or incomplete information is because they understand that it will be widely available to anybody, including stalkers, spammers, and phishers.

I think the Department of Commerce, which has an understandable interest in promoting accuracy, could advance that goal through support for better privacy.

Mr. BOHANNON. Thank you for your question, Congresswoman. I think it is our view that, as the MOU is reviewed and ICANN's commitments under the MOU are evaluated, I think those kinds of concrete things that ICANN under the existing arrangement has set out to do to improve accuracy and reliability need to be clearly documented, and I think as the MOU is renewed and reviewed, there may be a need to get more specific in terms of the Department of Commerce's expectations, and I think audits, random audits, is one example.

Ms. ALLEN. I agree there could be more that ICANN does in terms of positive reinforcement, proactive audits. There is more that others in the community, such as ISP's, could do, that could also help to stop the fraud.

Also, by having transparency, there is a self-policing effort, the fact that as consumers and/or businesses see there are fraudulent sites, report them and help to shut them down. That is part of the process as well.

Ms. KELLY. I noticed in some of the testimony, you were talking about the privacy of users and not the accuracy of information.

One of the questions I have is whether or not there should be a procedure in place of some sort so that people can appeal to the registrar on something that is a decision, some sort of a registrar decision on not to act on a false WHOIS data that is reported to it, because the registrar can make that choice right now.

It looks to me as though there is no penalty attendant to misinformation or to privacy theft at the present moment, in terms of whether or not the registrar acts.

I am wondering if we could again start with you, Mr. Rotenberg.

Mr. ROTENBERG. I think for the most part, the registrars have tried to stay out of the role of enforcing accuracy requirements. I think it could certainly be in the context of RAA's, which is the agreements that the registrars sign to sell the domain names, to impose accuracy requirements is one way to accomplish that goal.

As I said, I still think the privacy safeguards would work, because individuals would be less likely to provide inaccurate information.

Ms. KELLY. For anyone to plead a right to privacy, people need to remember there is no right to privacy on inaccurate information.

Mr. ROTENBERG. Congresswoman, if I may give an analogy, to the white pages and the phone books. I used to look at those. I was interested in how people protected their privacy in a very similar directory. A lot of people do not list their home address. A lot of women give a first initial instead of the complete first name.

You can say that is incomplete maybe, not inaccurate, but it is clearly done with the goal of protecting privacy.

I think some of that happens with the WHOIS directory as well.

Ms. KELLY. That is not misinformation. That was my point.

Mr. ROTENBERG. Okay.

Ms. KELLY. Mr. Bohannon?

Mr. BOHANNON. I think you are asking a very important question, Congresswoman. I think our view is that 3 years ago, ICANN made very specific commitments in these areas.

I think in my prepared remarks, I am very clear that while ICANN believes it has met those commitments, we feel they have really come up short.

They, in fact, did implement a process called the WHOIS data problem reporting system. It was supposed to address many of these questions.

As the GAO study found, it simply is not proving effective. The GAO found that less than a quarter of the complaints they filed—that they intentionally submitted and filed—were taken care of, and much of the misinformation or inaccurate information was never corrected.

Our view is that we have a framework in place. Let's make sure it is effectively enforced by ICANN and we do not have to go out and re-invent the wheel. Let's get the existing system working right. I think that does require some responsibility on the part of ICANN to do that.

Ms. KELLY. Do you think that penalties of some sort imposed by the Commerce Department might be of benefit there?

Mr. BOHANNON. I think my view is what we need to do is get ICANN to recognize that in its role, it needs to be in direct relationship with the registrars and use that relationship.

It needs to find, I think, a creative way, other than just de-certifying the registrar, which quite frankly right now is the only thing they can do. That may be too much of a response. We need to find some gradations here.

We are prepared in working with the registrars and all the communities of interest to find appropriate ways so that we can make these realistic commitments enforceable and workable and to everyone's interest.

Ms. KELLY. Thank you. Ms. Allen?

Ms. ALLEN. I wanted to distinguish between misinformation or inaccuracies with criminal intent, which I think that is why we want law enforcement and financial institutions to be able to have access to this information, to go after those players.

It is the second part of it, misinformation, that may be from marketing or a misrepresentation from a business point of view, but looking for responsibility in enforcement. There are some mechanisms in place that ICANN has not lived up to, and I think that is something that needs to be communicated in the contracts and MOUs.

Ms. KELLY. Thank you very much. My time is up, Mr. Chairman. Thank you.

Mr. PEARCE. I thank the gentlelady. The Chair notes that some members may have additional questions for this panel, which they may wish to submit in writing.

Without objection, the hearing record will remain open for 30 days for members to submit written questions to these witnesses, and to place the responses in the record.

I thank the witnesses from both panels. With that, this hearing is adjourned.

[Whereupon, at 2:02 p.m., the subcommittee was adjourned.]

A P P E N D I X

July 18, 2006

STATEMENT OF CHAIRMAN SPENCER BACHUS
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
"ICANN AND THE WHOIS DATABASE; PROVIDING ACCCESS TO PROTECT CONSUMERS FROM PHISHING"
JULY 18, 2006

Good morning. The subcommittee will come to order. At today's hearing we will focus on proposals before the Internet Corporation for Assigned Names and Numbers (ICANN) that would limit the public's access to domain name registrant contact information via the Whois database. This would put many long-standing and valuable uses of this data off-limits and could make it difficult for law enforcement and financial institutions to identify and bring down the perpetrators of online financial fraud.

It has always been ICANN's policy that certain contact information for registrants of Internet domain names in dot-com and other generic top level domains is collected and made available to the public. This policy helps to promote accountability online, since consumers, financial regulators and others can consult this data through a service called Whois – in seeking to determine who or what entity is responsible for a particular website or other online location.

There are many essential and legitimate uses of the current Whois database. In the wake of Hurricane Katrina, the American Red Cross used the Whois database to shut down dozens of unauthorized Web sites that were soliciting money under the Red Cross logo. EBay's investigators use the Whois database hundreds of times a day to pursue scamsters.

More generally, consumers may rely on the Whois database to know more about who they are dealing with online; parents may rely on the Whois database to look into who is operating websites which their children visit; and law enforcement agencies may rely on the Whois database to investigate crimes. Moreover, millions of businesses use the Whois database every day to identify cyber squatters, track down those conducting piracy or product counterfeiting over the Internet, and to investigate online scams.

Financial institutions – which are the focus of this hearing -- use Whois data to respond to identify theft and account fraud particularly as it relates to "phishing." The financial services industry is currently battling "phishing" scams at an unprecedented level. Phishing refers to a practice where someone misrepresents their identity, typically claiming to be from a financial institution or Internet Service Provider (ISP), in order to trick a consumer into providing sensitive personal information over the Internet. Typically, the e-mail directs the person to a website that mirrors the legitimate business' website and asks the person to enter a credit card number, a bank account number, social security number, or other sensitive personal information under the guise that the information is needed for identity or account verification, account continuance, or account restoration. In reality, the e-mail or website is controlled by a third party who is attempting to extract information that will be used in identity theft or other fraudulent ways.

Over the last few years, the number and variety of phishing attacks has become widespread. In May 2006, the Anti-Phishing Working Group – which is comprised of financial institutions, ISPs, and law enforcement --

reported nearly 12,000 phishing sites which on average remained online for 5 days. These sites "hijacked" the brand of 137 companies in an attempt to fraudulently gain access to sensitive consumer information. The vast majority of these phishing sites hijacked the brands of financial services companies. A May 2005 consumer survey by First Data found that 43 percent of respondents had received a phishing attack, and of those 5 percent – about 4.5 million people – provided their personal information. Nearly half of the phishing victims, 45 percent, reported that their information was used to make an unauthorized transaction, open an account, or commit another type of identity theft. And according to a survey conducted by Gartner, Inc., direct losses from identity theft fraud against phishing attacks victims cost U.S. banks and credit card issuers about $1.2 billion in 2003.

Notwithstanding all of these critically essential and legitimate uses of the Whois database, ICANN is actively considering a policy change to restrict Whois data to those who resolve "technical issues." If this change is adopted, most of the data now in the Whois database would be cut off from public access – perhaps including data as fundamental as the name of the domain name registrant.

I am concerned that proposals limiting the use of the information for resolving "technical issues" will make it difficult for financial institutions to respond to identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect financial institutions and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the Whois

contact information. Such uses of Whois data would become slower, more difficult and expensive, and even impossible, were ICANN to shift its policy as it now being proposed. I shared this concern with Secretary of Commerce Carlos Gutierrez in April and remain concerned today. I hope today's hearing will shed some light on this issue and look forward to hearing from the witnesses.

The chair now recognizes the Ranking Member of the Subcommittee, Mr. Sanders, for any opening statement that he would like to make.

Opening Remarks
Representative Maxine Waters D-CA 35th

Subcommittee on Financial Institutions and Consumer Credit

Hearing on

"ICANN and the Whois Database: Providing Access to Protect Consumers from Phishing"

Tuesday, July 18, 2006

Good Morning. Mr. Chairman. Ladies and Gentlemen. I want to thank Chairman Bauchus and the Ranking Member Mr. Sanders for holding today's hearing on ICANN and the Whois Database: Providing Access to Protect Consumers form Phishing."

It seems as if a day does not go by without something appearing in the media about data security and consumers. This is a timely hearing if for no other reason than the

continued importance of protecting consumers from invasions of their privacy as well as the outright theft of their personal information. With the growth of the Internet and technological advances giving just about everyone more access to our personal records it is no wonder that "phishing" has become a buzzword. The Internet has spawned a whole new generation of persons often masquerading as someone else who through coercion or trick acquire our most sensitive information -- social security numbers, bank accounts and credit card information.

What really concerns me is that these predators often a prey on senior citizens and the unwary. While many of us consider ourselves computer savvy, it only takes a few seconds and anyone can become vulnerable. There are

sophisticated operations set-up outside of the United States as well as those operating here that allow individuals to believe that they are dealing with a bona fide business entity when in fact it is an imposter ready to pounce at the opportunity to take information and use it to their gain. One report identified 12, 000 phishing sites. Guess what, they are here today and gone tomorrow, since most only stay up and running on average for 5 days.

There are several tools that can be used to prevent fraud on the Internet. One of those tools is the Whois database, which is credited with pulling non-bona fide sites from the Internet. However, there is an issue about who should have access to the Whois database. Should access to Whois be limited, or should there be access to many? This hearing should shed light on this question. It is certainly an

important issue because it is a primary tool designed to prevent fraud on the Internet that victimizes consumers. Aside from anti-fraud education and outreach programs at the state and local level such as those in California, we are at the mercy of predators. Madame Chairwoman. Thank you.

STATEMENT

OF

CATHERINE A. ALLEN
CEO, BITS

BEFORE THE

UNITED STATES CONGRESS
HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

HEARING ON

ICANN AND THE WHOIS DATABASE: PROVIDING ACCESS TO PROTECT CONSUMERS FROM PHISHING

JULY 18, 2006

TESTIMONY OF CATHERINE A. ALLEN
CEO, BITS

Introduction

Good afternoon Chairman Bachus, Ranking Member Sanders, and members of the Subcommittee. My name is Catherine Allen. I am the Chief Executive Officer of BITS.

I am pleased to appear before you today on behalf of BITS and our member financial institutions with respect to the topic of a proposed change to the WHOIS data base within the Internet Corporation for Assigned Names and Numbers, ICANN. Thank you, Chairman Bachus, for meeting with executives from AmSouth and BITS earlier this year on this issue.

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. We are the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS' member companies provide fuel for America's economic engine, accounting directly for $50.5 trillion in managed assets, $1 1 trillion in revenue, and 2.4 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues for the financial services industry. We focus on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety and soundness of financial payments systems and services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses. Working Groups share successful strategies and best practices for managing risks, reducing fraud, managing IT service provider relationships, facilitating communications in times of crisis, and addressing risks in the changing payments environment. We produce a host of publicly-available documents that serve as a repository of best practices and guidelines, available on the BITS web site at www.bitsinfo.org.

Especially relevant to today's testimony, the mission of the BITS Fraud Reduction Steering Committee (FRSC) is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve. Equally relevant is the BITS Security and Risk Assessment Steering Committee, the group that first raised issues of concern about proposed

changes to the ICANN WHOIS data base, and its purpose. The BITS Security and Risk Assessment Steering Committee and Working Group include senior executives responsible for information security among the nation's largest financial institutions. Both groups are deeply concerned about changes to the WHOIS data base that might increase fraud and reduce information security.

BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators and the Federal Reserve, as well as technology associations along with third-party service providers to achieve our mission.

BITS is also a founding and active member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). The mission of the FSSCC is to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and ID theft. While fraud reduction and deterrence works, there are still victims of financial crimes. As just one example of proactive customer assistance, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, recently announced that it had helped over 6,000 individuals in restoring their financial identity. ITAC is important and is a landmark cooperative effort. While identity theft actually occurs infrequently, its effects are very serious for those who experience it. ITAC's services are provided free of charge to victims who are referred by ITAC members.

As part of BITS and our member company efforts to reduce fraud and address information security challenges, BITS is working with members and Internet Service Providers (ISPs) on an email security project. The goal of the project is to enhance the security of electronic mail communications and reduce the amount of spam, phishing and malicious code. We are striving to:

- Ensure confidentiality of information exchange among financial institutions, as well as with customers and clients;
- Protect customers and their accounts from identity theft and account fraud; and

- Restore the reliability of the e-mail delivery channel for financial institutions.

The key components of this e-mail authentication project include:

- Outlining the problem and how this project is important for the financial services industry;
- Seeking agreement within the financial services industry on the protocols/standards and a strategy for implementation;
- Engaging key Internet Service Providers (ISPs) and other important stakeholders from the vendor community; and
- Developing a strategy for communicating this effort with media, regulators and policy officials.

With the growth of the Internet and its fundamental role as a foundation for electronic commerce, including financial services, the role of the ICANN and its significance has grown exponentially. It is therefore with great concern that our member institutions have become aware of a proposed change in the type of information to be collected and maintained in the ICANN's WHOIS database. ICANN, as you know, is a non-profit corporation responsible for IP address space allocation, Top Level Domain Name management, and other functions. The WHOIS database gives information about domain names and the IP addresses associated with domain names. Three types of information are available:

- **Registrant Contact**—includes who registered for the domain name/IP address; who owns the name; who paid for the name; and the owner's name and address.
- **Administrative Contact**—includes who to call for administrative and billing information, and their name, phone number, address and email address; and
- **Technical Contact**—this specifies who to call if there is a problem with the web site.

As part of their efforts to combat fraud, financial institutions are constantly watching for incidences of domain name fraud, what we sometimes refer to "cyber squatting," or "typo squatting". People frequently register domain names that are similar to those used by financial institutions. Our customers and other Internet users may inadvertently access these fraudulent sites due to a lack of knowledge about the financial institution's actual website name and location or it may happen when a person mis-keys the domain name. In one case, a financial institution found a web site with a name that was identical to its own, except that one vowel in the name was missing. An individual going to this web site saw a home page with the financial institution's name and numerous advertisements for off-shore checking accounts, loans, and mortgages. Not only is this an example of the theft of

intellectual property, but it also potentially exposes the customer to products that may not even be offered by financial institutions at all and creates a risk to the consumer.

Using the ***Registrant*** Information from WHOIS, the financial institution in this instance was able to contact the web site owner and subsequently sent a cease and desist letter to have the site removed.

One of the key uses of the WHOIS data is for shutting down phishing sites. As part of investigating phishing incidents, financial institutions sometimes discover that a legitimate web site has been taken over by phishers, without the web site owner's knowledge. In this scenario, it frequently takes the cooperation of the WHOIS ***technical*** contact, the WHOIS ***registrant*** contact, and the hosting site to get the phishing site shut down.

In early 2006, a financial institution discovered that it was being phished from a site in Taiwan. Efforts to have the web site shut down using the ***technical*** contact information were not successful. The ***full*** WHOIS information was provided to the US Secret Service and the Taiwanese police who made local contact with the web site owner and the ISP and got the phishing site shut down.

These are just two examples of the reasons that financial institutions find the WHOIS data base so important as a tool for fighting fraud and protecting the public.

All of the WHOIS information is currently freely available to anyone with Internet access. While it may be prudent to restrict some access to Registrant and Administrative information in order to protect the privacy of individuals from literally anyone being able to access it, a right balance is needed. In contrast with the general public who most often do not have a need to know all of the information that is available in the WHOIS data base, we believe it is paramount for financial institutions to maintain unrestricted access for purposes of preventing and reducing incidences of fraud.

BITS submitted a comment letter on this subject in April of 2006, has met directly with ICANN officials, and is continuing to interact with ICANN leadership to make clear the importance of maintaining the ICANN WHOIS database in a manner that will continue to allow financial institutions to use the database to deter and prevent fraud. A copy of our letter is attached for the record.

Other organizations have also submitted letters to ICANN in support of continued open access to the WHOIS data base, including the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC); the American Intellectual Property Law Association; the International Anticounterfeiting Coalition; and the American Hotel and Lodging Association.

As you are aware, a January 18, 2006 ICANN WHOIS Task Force report contained two opposing formulations of the "purpose of WHOIS."

Under formulation 1, the only purpose of WHOIS is to "resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver" (i.e., narrow technical issues). Under formulation 2, the purpose of WHOIS is to help resolve a broader range of "technical, legal or other issues regarding registration or use of a domain name." **We believe the adoption of formulation 1 would make it more difficult and time-consuming for financial institutions to identify and stop domain-based scams and the identity theft and account fraud that result.**

Further, financial institutions must also deal with other domain-based issues including, but certainly not limited to, trademark infringement, unauthorized and sometimes unlawful disclosure of confidential, proprietary or customer information, spam attacks, inappropriate content sent or received via email, staff harassment/stalking, and violation of intellectual property rights by web site operators. While our members' foremost concern is to protect their customers and maintain their trust, they must also be mindful of the need to comply with the requirements set forth by numerous laws, regulations and supervisory guidance.

We believe that formulation 1 (or other efforts to limit or narrow the information) in WHOIS could adversely affect the financial services industry's efforts to respond identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Often times, the fraudsters will register a domain name in the name of innocent consumers without the knowledge of the consumer. In most instances, it is not until these unsuspecting consumers are contacted by the financial institution that they learn they may have been a victim of identity theft, giving them the opportunity to remedy the effects of identity theft sooner rather than later.

In addition, most innocent victims have been and continue to be extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is a target or potential target of a phishing attack. Also, agreement from the operators to take down websites quickly when there is clear violation of trademarks or indications of fraud is only a partial solution. Financial institutions still need the WHOIS information to address the other forms of abuse noted above.

For these reasons, we have urged ICANN to adopt Formulation 2.[1] Formulation 2 will provide financial institutions with the information they need to respond to identity theft and account fraud.

It should be noted that on June 20, an official statement of the US government was submitted to ICANN, also in support of Formulation 2.

It is our understanding that during recent ICANN meetings, June 24 – 30, in Marrakech, the decision to choose between Formulations 1 and 2 was essentially postponed, for further deliberation and discussion. The WHOIS Task Force is to issue a report in October, followed by a one-month comment period, then a vote will be held in December, to be followed by Board action in January 2007.

On behalf of BITS and our member financial institutions, recognizing that the ICANN Board is the ultimate decision maker on these matters, **we encourage Congress to support strongly the adoption of Formulation #2.**

Thank you for the opportunity to testify before you today. I would be happy to answer any questions.

[1] http://www.icann.org/announcements/announcement-18jan06.htm)

Overview of BITS' Activities Related to ICANN's WHOIS Data Base
March – July 2006

On March 14, 2006, the BITS Security and Risk Assessment (SRA) Working Group discussed the implications of a proposal to restrict information in the WHOIS database. The SRA agreed to develop a comment letter to the Internet Corporation for Assigned Names and Numbers (ICANN).

On April 14th, BITS submitted a comment letter based on input from SRA members and the BITS Fraud Reduction Steering Committee to the Internet Corporation for Assigned Names and Numbers (ICANN) expressing support for "formulation 2" of the WHOIS database.

On April 17th, BITS forwarded the comment letter to the following individuals:

- Don Donahue of DTCC and George Hender of the Options Clearing Corporation, the outgoing and incoming leadership of the Financial Services Sector Coordinating Council (FSSCC).
- Scott Parsons, Deputy Assistant Secretary of Treasury and chair of the Financial and Banking Infrastructure Information Committee (FBIIC).
- Several officials in the Commerce Department's National Telecommunications and Information Assurance office.

In response to the comment letter, BITS staff received an e-mail from Vint Cerf (ICANN Chairman and one of the founders of the Internet) and a call from John Jeffrey, General Counsel for ICANN.

BITS staff briefed the Roundtable's Government Affairs Council on April 26 and briefed Roundtable Government Affairs staff on May 12.

On May 3, AmSouth officials briefed Rep. Spencer Bachus, Chairman, Subcommittee on Financial Institutions and Consumer Credit. AmSouth officials also discussed this issue with the staff of Senator Richard Shelby, Chairman of the Senate Banking Committee.

On May 16, Dr. Paul Twomey, President of ICANN and John Jeffrey, General Council of ICANN, briefed the BITS Advisory Council on a conference call. In addition, AmSouth officials and BITS staff prepared a presentation for the BITS Advisory Council outlining the key issues and concerns and BITS and member efforts to raise awareness.

On May 16, AmSouth officials met with senior Treasury Department officials.

On May 23, BITS staff reached out to other associations such as the SANS Institute to ensure that other security-focused organizations were aware of the issue.

On May 31, BITS staff participated in a conference call with other industries and organizations that have an interest in retaining the WHOIS data base. The meeting was hosted by Steve Metalitz, Counsel for the Coalition for Online Accountability.

On June 2, BITS hosted a conference call of an interagency working group whose members are involved in developing the Administration's policy on ICANN-related issues. Representatives from the following agencies participated: Federal Trade Commission, Federal Bureau of Investigation, Internal Revenue Service, and Commerce Department.

On June 6, BITS staff briefed the Financial Services Sector Coordinating Council (FSSCC) and the Financial and Banking Infrastructure Information Committee (FBIIC) on the ICANN WHOIS issue. The FSSCC agreed to develop and submit a joint comment letter to ICANN and the Government's interagency working group.

On June 22, the chairman of the FSSCC submitted a joint comment letter from all the associations representing the financial services sector to the ICANN leadership and the representatives of the Government's interagency working group.

From June 24 – 30, in Marrakech, Morocco the ICANN Board met to choose between Formulation 1 and 2. The decision to choose between Formulations 1 and 2 was essentially postponed, for further deliberation and discussion. The WHOIS Task Force is to issue a report in October, followed by a one-month comment period, a vote in December, with action by the ICANN Board scheduled for January 2007.

On July 5, BITS received a request to testify before the House Financial Services Subcommittee on Financial Institutions on Tuesday, July 18th on the subject of "ICANN and the WHOIS Database: Providing Access to Protect Consumers from Phishing."

On July 18, BITS CEO Catherine A. Allen, provided testimony.

BITS
FINANCIAL SERVICES
ROUNDTABLE

1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

April 14, 2006

To: Internet Corporation for Assigned Names and Numbers

e-mail address: <whois-comments@icann.org>

Re: WHOIS Data Base

Dear Sirs and Madams:

The purpose of this letter is to comment on the proposal before the Internet Corporation for Assigned Names and Numbers (ICANN) to limit the type of information collected and maintained in the WHOIS data base. Based on a review of the information provided in the January 18, 2006 task force report containing two opposing formulations of the "purpose of WHOIS," and discussions among information security and fraud risk managers, we urge ICANN to adopt Formulation 2.[1] Formulation 2 will provide financial institutions with the information they need to respond to identity theft and account fraud. In addition to commenting on the two proposals, we want to outline the activities of BITS and our members in addressing information security and identity theft challenges.

Under formulation 1, the only purpose of WHOIS is to "resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver" (i.e., narrow technical issues). Under formulation 2, the purpose of WHOIS is to help resolve a broader range of "technical, legal or other issues regarding registration or use of a domain name." We believe the adoption of formulation 1 would make it more difficult and time-consuming for financial institutions to identify and stop domain-based scams and the identity theft and account fraud that result.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. Further, financial institutions must also deal with other domain-based issues including, but certainly not limited to, trademark infringement, unauthorized and sometimes unlawful disclosure of confidential, proprietary or customer information, spam attacks, inappropriate content sent or received via email, staff harassment/stalking, and violation of intellectual property rights by web site operators. While our members' foremost concern is to protect their customers and maintain their trust, they must also be mindful of the need to comply with the requirements set forth by numerous laws, regulations and supervisory guidance.

[1] http://www.icann.org/announcements/announcement-18jan06.htm)

We believe that formulation 1 (or other efforts to limit or narrow the information) in WHOIS could adversely affect the financial services industry's efforts to respond identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Often times, the fraudsters will register a domain name in the name of innocent consumers without the knowledge of the consumer. In most instances, it is not until these unsuspecting consumers are contacted by the financial institution that they learn they may have been a victim of identity theft, giving them the opportunity to remedy the effects of identity theft sooner rather than later. In addition, most innocent victims have been and continue to be extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is a target or potential target of a phishing attack. Also, agreement from the operators to take down websites quickly when there is clear violation of trademarks or indications of fraud is only a partial solution. Financial institutions still need the WHOIS information to address the other forms of abuse noted above.

About BITS

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS' member companies provide fuel for America's economic engine, accounting directly for $50.5 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Within BITS there are two working groups that have an interest in the WHOIS data—the information security experts who are involved in the BITS Security and Risk Assessment Working Group and the fraud reduction experts who are involved in the BITS Fraud Reduction Steering Committee (FRSC). The mission of the SRA is to strengthen the security and resiliency of financial services by a) sharing and developing best practices to secure infrastructures, products and services; b) maintaining continued public and private sector confidence; and c) providing industry input to government agencies and regulators on policies and regulations. The mission of the FRSC is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

Efforts to Strengthen Cyber Security, Reduce Fraud and Mitigate Identity Theft

The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud

and identity theft. As just one example of these efforts, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, announced in March that it had helped over 5,000 individuals to restore their financial identity. These services are provided free to consumers by ITAC members.

We have included a detailed summary of BITS' efforts to address information security, fraud reduction and critical infrastructure protection in the appendix.

While we understand that the public comment period officially closed on February 8, 2006, we are hoping that ICANN will consider this input from information security and fraud risk experts of the largest financial services companies who are the "front lines" of the identity theft and Internet fraud battlefield. If you have any further questions or comments on this matter, please do not hesitate to contact me or John Carlson at john@fsround.org or 202-289-2442.

Sincerely,

Catherine A. Allen
CEO, BITS

Appendix: Protecting the Critical Infrastructure: BITS' Accomplishments in 2005

BITS
FINANCIAL SERVICES
ROUNDTABLE

APPENDIX: PROTECTING THE CRITICAL INFRASTRUCTURE: BITS' ACCOMPLISHMENTS IN 2005

PUBLICATIONS OF BEST PRACTICES AND GUIDELINES

Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy

- The BITS study on "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy" outlines inefficiencies resulting from regulatory overlap within:
  - The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA);
  - The Gramm-Leach-Bliley Act of 1999 (GLBA);
  - The Sarbanes-Oxley Act of 2002 (SOX); and
  - The proposed U.S. Inter-agency Operational Risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) for Regulatory Capital (applying the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also referred to as Basel II), July 2003.
  - The study includes specific recommendations for implementation by member institutions to increase efficiencies, and further provides recommendations for regulators to work with the financial services industry to reduce unnecessary burdens and eliminate inconsistent requirements. The study was made available in hard copy and jointly distributed by BITS and the Roundtable to key regulators as well as member institutions in a public launch event held October 11.

BITS Consumer Confidence Toolkit and Voluntary Guidelines

- BITS has developed a *Consumer Confidence Toolkit: Data Security and Financial Services.* This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS has developed Voluntary

Guidelines as recommendations to member institutions for managing information security and consumer confidence issues.

Protecting the Elderly and Vulnerable

- BITS released a new tool in October 2005 to help reduce fraud. The publication, "BITS Fraud Protection Guide: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation," describes the growth of this fraud, highlights ways to detect and prevent it, and urges financial institutions to work proactively to reduce it. "This new BITS publication serves to protect some of our nation's most vulnerable populations and reinforces our member institutions' 24/7 commitment to safe and secure financial transactions," said BITS CEO Catherine A. Allen. In the coming months, BITS will release a toolkit for educating financial center and loss management personnel on ways to identify and prevent this type of financial crime. The Financial Services Industry Toolkit provides information to support the implementation or improvement of a financial institution internal prevention program for education and awareness to protect the elderly and vulnerable from financial fraud.

E-Scams

- BITS formed a subcommittee under the auspices of the Internet Fraud Working Group to address the various scams operating throughout the Internet today. The BITS e-Scams Subcommittee was comprised of e-commerce specialists from more than 30 financial institutions. The e-Scams Subcommittee's goal was to provide information and best practices to BITS members and the financial services community in order to protect customers and enhance confidence in the Internet as a medium for online financial services. The result is a Members Only document that: defines the current landscape; assesses the impact of e-scams on financial institutions; reviews current industry technology solutions; provides an overview of an e-scam program with an emphasis on e-scam investigations; discusses outsourcing e-scams management; and outlines internal and external education and awareness programs. A final document is due for release in December 2005.

Back-Up Power Issues

- The *BITS Guide to Business-Critical Enterprise Power* (the *Guide*) is in draft. It provides financial institutions with industry business practices for understanding, evaluating and managing risks if the availability of the electrical system is disrupted. Further, it outlines ways financial institutions can enhance reliability and ensure uninterrupted back-up power, referred to as "enterprise power." The *Guide* is written for interested parties—from CEOs to business managers, risk managers to business continuity professionals, procurement experts to facilities managers—as they analyze risks, conduct due diligence for enterprise power and integrate evolving regulatory and building code requirements into business continuity plans. The final Guide will be available early in 2006. The full draft, completed in 2005, is being used and vetted currently.

BITS Critical Success Factors for Security Awareness & Training Programs

- Under the auspices of the BITS Security and Risk Assessment Program, BITS developed a description of critical factors for establishing and maintaining a comprehensive security awareness and training program for financial institution personnel. Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice.

BITS Key Considerations for Global Background Screening Practices.

- BITS released the *BITS Key Considerations for Global Background Screening Practices* on June 29, 2005. This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The paper is divided into three sections:
  - Overview of the financial industry's legal and regulatory requirements;
  - Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
  - Information to validate identity and background, listed by country.
- Each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements. The paper is available on the BITS website at www.bitsinfo.org on the publications page.

Key Contractual Considerations for Developing an Exit Strategy

- Published in May, 2005, the *BITS Key Contractual Considerations for Developing an Exit Strategy* provides detailed suggestions for contracts with third party service providers. For all critical infrastructure companies, developing an exit strategy at the onset of the relationship can help the organization effectively manage risk and ensure continuity of service.

Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act

- This paper provides informed analysis of the risks and benefits associated with implementation of the Check 21Act. Strategies for mitigating risks are included as well as a matrix that describes Check 21-related risks and mitigants from the standpoint of three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank.

Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments

- Loan fraud is a fast-growing problem. This Members' Only guide helps financial institutions catch loan frauds as they happen and recover from related losses. Members interested in obtaining a copy may access it via the BITS site, www.bitsinfo.org, in the Members Only area.

BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings

- In January 2005 BITS published the *BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings.* This Members' Only guide assists financial institutions in understanding technology to verify and authenticate online users and determine the level of risk users pose to the institution. This document was created to help financial institution fraud managers as they explore these technologies and identify those that may be appropriate for their needs. This paper focuses on technology solutions for:
  - Verification. These products screen data elements provided by a client to ensure the elements (Social Security numbers, addresses, etc.) are real.

- Authentication. Once the data elements are verified, authentication products ensure the credentials given belong to the person providing them.
- Financial experience information. Having verified the data elements and authenticated the customer, financial experience information determines the level of risk assumed by accepting the potential customer.

BITS Kalculator: Key Risk Management Tool for Information Security Operational Risks

- The *Kalculator* starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the *Kalculator*, financial institutions score their information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. Companies can use the results to boost their ability to assess and mitigate risks. The *Kalculator* is unique in that it brings together information security risk categories from international security standards and emerging operational risk regulatory requirements into one tool that can be easily customized.

Developing a KRI Program: Guidance for the Operational Risk Manager

- The document, *Developing a KRI Program: Guidance for the Operational Risk Manager*, helps operational risk managers establish and maintain strong KRI programs in an environment of increased operational risk regulation.

Best Practices in Patch Management for the IT Practitioner

- *BITS Best Practices in Patch Management* provides critical recommendations for an enterprise approach to managing patches. Divided into 10 sections reflecting the components of effective patch management processes, the document provides considerations for defining roles, responsibilities and tools; developing and maintaining an inventory of IT infrastructure; developing a "standard build"; and verifying patch installation. While created for financial institutions, these recommendations may be applied to other industries.

BITS IT Service Providers Expectations Matrix

- The BITS *IT Service Provider Expectations Matrix* provides financial institutions, service providers, and audit and assessment organizations with comprehensive and consistent expectations to reduce risk. Presented in an Excel spreadsheet, it outlines financial institution expectations for the security of information and personnel, as well as policies and processes for ensuring physical security. The expectations address critical disaster recovery/business continuity issues necessary to ensure products and services are supported by and coordinated with service providers.

BITS Guide to Business-Critical Telecommunications Services

- On November 15 of 2004, BITS released the *BITS Guide to Business-Critical Telecommunications Services*, however it has received continued use and additional visibility in 2005, including as a helpful tool in the aftermath of Hurricanes Katrina, Rita and

Wilma. The *BITS Guide* highlights questions business continuity planners and other risk managers should ask themselves as well as an overview of key points to consider in risk assessment, due diligence, contracting, testing and monitoring processes of their telecommunications services.

COMMENT LETTERS

Comment Letter on FDIC Study, "Putting an End to Account-Highjacking Identity Theft"

- BITS, The Financial Services Roundtable and the Identity Theft Assistance Corporation jointly submitted a comment letter, raising concerns about the proposed approach to remedies for fraud-related security risks. The study did not adequately take into account the fact that financial institutions are applying a risk-based approach for evaluating the risks, deploying controls and offering convenient solutions to their customers and recommended solutions that are complex, unwieldy, and, in some instances, will not provide the intended remedy.

Comment Letter on Department of Homeland Security (DHS) Interim Rule on Procedures for Handling Critical Infrastructure Information

- BITS and The Financial Services Roundtable submitted a comment letter to DHS on a rule to establish "uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security." The letter outlines concerns about the scope and implementation of the procedures. It states that DHS must implement robust controls to adequately protect employees and customers of financial institutions.

TESTIMONY

Hearing on "Continuity of Operations in the Financial Services Sector Post a Major Event," to the House committee on Government Reform Subcommittee on Government Management, Finance, and Accountability

- On September 26, BITS CEO Catherine A. Allen testified at a field hearing in New York City on the current status of financial market preparedness for wide-scale disasters and disruptions. The hearing was held by the House Committee on Government Reform Subcommittee on Government Management, Finance, and Accountability. Cathy's testimony focused on actions the financial services sector has taken in response to the 9/11 terrorist event and natural disasters such as Hurricanes Katrina and Rita. She praised the financial services' sectors preparedness and responsiveness and offered recommendations for additional steps that need to be taken by the Federal government and all critical infrastructure sectors. Cathy made specific recommendations for maintaining diverse and resilient communications channels, investing in the power grid, recognizing the dependence of all critical infrastructures on software operating systems and the Internet, and improving coordination among all critical infrastructures and with federal, state, and local government when events occur. She emphasized the importance of addressing the interdependence of all critical infrastructure sectors. Those of greatest concern to the financial services sector are interdependencies with telecommunications, energy and transportation sectors. For access to Cathy's full testimony, go to http://www.bitsinfo.org/p_public_testimony.html.

"The Department of Homeland Security Cybersecurity Enhancement Act of 2005" to House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

- Catherine A. Allen, BITS CEO, testified in April, 2005 on the importance of elevating the position of Cybersecurity Director at the Department of Homeland Security to an Assistant Secretary level. Her testimony included a description of the current cybersecurity landscape, and what BITS and the industry are doing to address threats. The testimony also included the BITS recommendations to the government to strengthen cybersecurity, referred to in detail and presented as the acronym PREPARE©.

SUMMITS, FORUMS AND CONFERENCES

Critical Infrastructure Protection

- BITS CEO Catherine A. Allen participated as one of four panelists at an event convened by George Mason University's Critical Infrastructure Protection Program at the National Press Club on November 29, 2005. Award-winning journalist Frank Sesno moderated the panel, "After the Storms, Repairing the Damage." James Lee Witt, former FEMA Director, keynoted the event. Other panelists were Dennis Barbour, Mayor of Carolina Beach, NC and J. Michael Hickey, Verizon. Catherine drew on lessons learned by the financial services sector, and stressed the continuing need to address issues of interoperability, interdependence with other sectors, implementation of lessons learned, and consumer confidence.
- BITS Senior Director John Carlson participated in the Vanderbilt University-hosted US Japan Critical Infrastructure Protection Forum on November 29 and 30, 2005 in Washington, DC. John spoke about BITS' efforts in cross-sector coordination among critical infrastructure sectors and cybersecurity and participated in a panel discussion on business continuity planning and response from a multi-day regional power outage scenario. The forum fostered dialogue between US and Japanese industries on how best to protect infrastructures that support those nation's economies. Speakers included senior US and Japanese government and private-sector officials and experts in financial services, information technology, power, telecommunications and transportation. For more information, contact John Carlson, john@fsround.org.
- John Carlson represented BITS at three meetings on July 11, August 12 and September 30, 2005 with senior Department of Homeland Security officials and over a dozen associations representing the business, IT and telecommunications industries. The purpose of the meetings was for the Department of Homeland Security to get input and recommendations from association leaders who are active in cyber security issues and to discuss how best to assess cyber security risks, improve the public/private partnership, expand information sharing, and develop public and private incentives to encourage government and the private sector to enhance cyber security.
- On June 17, 2005 Dartmouth's Institute for Information Infrastructure Protection (I3P) hosted a forum on "Financial Services Challenges in the Cyber World" at New York University in New York City. BITS participated in a panel discussion along with representatives from BITS member companies and key federal government agencies. Approximately 25 government and academic leaders involved in research on cyber security and critical infrastructure issues participated in the meeting.

- BITS held conference calls with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS disseminated daily updates to members beginning on September 1, serving as a repository and conduit for timely information. BITS worked closely with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and disseminated key information to our members from regulatory agencies, Treasury and the Department of Homeland Security. Topics included assessment of impacts from the storm, efforts to deliver adequate cash supplies, FEMA's distribution of debit cards to victims of Katrina, talking points for consumer assistance, guidance from regulatory agencies, and important contacts for additional support. BITS also helped develop a press release that was issued by the FSSCC and outlined the sector's efforts to respond to the crisis. This information-sharing and coordinating role continued through Hurricanes Rita and Wilma on an as-needed basis. BITS also worked with the FSSCC to develop a memo on lessons learned from the Hurricanes that was send to Treasury and the FBIIC.

A Strategic Look at Authentication

- On March 8, 2005, BITS hosted a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum focused on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

BITS Regulatory Forum

- The BITS Regulatory Forum was held on April 26, 2005 and established a dialogue among regulators and financial services firms on the impact of regulatory requirements and supervisory processes. Many of those requirements relate to critical infrastructure protection and security issues. Participants reviewed steps to be taken by all parties to increase efficiency in the regulatory and supervisory process. Senior level regulators and BITS members took part in this session, the first step in an iterative, cross-sector process. The Forum was the first public release of the study, developed on BITS' behalf by KPMG, "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy"

BITS/American Banker Financial Services Outsourcing Conference

- The Fourth Annual BITS/American Banker Outsourcing Conference, presented with The Santa Fe Group in 2005, was held on November 7 - 8 at the Renaissance in Washington D.C. This year's agenda followed four key themes:
  - Governance: Best practices of financial institutions and service providers.
  - Compliance: Strategies for negotiating the current landscape and requirements for privacy and security.
  - Risk Management: Strategies, controls and processes to coordinate risk management across the enterprise.
  - Change: Practical guidance for managing today's dynamic relationships.

POLICY DEVELOPMENT

NOTE: BITS serves as a source of fact-based information in the development of policy positions. Following are recent examples, resulting either in a formal position from both BITS and The Financial Services Roundtable, or indirectly, through participation in national-level councils, working groups and task forces. Other examples of BITS' role in policy development are listed above in the categories of Comment Letters and Testimony.

- Joint BITS and Financial Services Roundtable Policy on Authentication Mandates
- Joint BITS and Financial Services Roundtable Policy on Spyware
- Joint BITS and Financial Services Roundtable Policy on Software Security
- Joint BITS and Financial Services Roundtable Policy on Internet Fraud and Phishing
- Support for President's National Infrastructure Advisory Council (NIAC)
- Participation in National Security Telecommunications Advisory Council (NSTAC) Financial Services Task Report
- Participation in Network Reliability and Interoperability Council (NRIC) VII
- Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG)
- Participation in the National Cyber Security Partnership

PILOTS AND PROJECTS

Financial Institutions Shared Assessments Project (FISAP)

- BITS has recently launched a new project aimed at improving efficiencies and achieving cost savings related to assessments of shared third party services providers. This Financial Institutions Shared Assessment Project (FISAP) is in pilot stage.
- Six institutions formed FISAP to leverage the *BITS Framework* and *BITS Expectations Matrix* and develop an industry solution for service provider assessments. Big Four firms are acting as Technical Advisors to the project. Critical success factors are to:
  - Develop reports that are comprehensive and suitable for multiple financial institutions;
  - Reduce the time and resources financial institutions and service providers spend responding to and executing one-off assessments to verify controls and security;
  - Create a process that is repeatable and consistent; and
  - Encourage support of regulators.
- The project is intended to result in significant cost savings and efficiency gains. These "shared assessments" are being developed to improve assessments based on consistent and objective information that is provided through a regularly-updated, standardized questionnaire as well as third-party testing and objective reporting on controls. It should be noted that FISAP is not a "100%" solution. The savings and efficiencies will fluctuate by risk, service and amount of dedicated vs. shared services. BITS expects to expand this project to additional participants in early 2006.

Anti-Phishing Efforts

- BITS is responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams,

BITS created a Phishing Prevention and Investigation Network. The BITS Phishing Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The BITS Phishing Network includes a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network also provides data on trends to help law enforcement build cases and shut down identity theft operations. The BITS Phishing Prevention and Investigation Network:

- Helps member institutions monitor and shut down e-scams faster and more effectively.
- Reduces financial institution manpower costs and losses.
- Increases phishing investigations and arrests of perpetrators.
- Facilitates communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

ChicagoFIRST

- With the encouragement of the US Treasury and support from BITS, Chicago's premier financial services institutions formed ChicagoFIRST in July 2003 as an industry coalition that addresses homeland security issues requiring a common response by Chicago's financial services sector. In 2005, ChicagoFIRST became a model for a similar regional coalition in Florida. These initiatives are prompted by a consensus that existing activities at the regional level do not adequately address the critical infrastructure protection concerns of Chicago's financial institutions. The mission of ChicagoFIRST is:
  - To increase the resilience of the Chicago financial services industry in the event of a regional disaster in collaboration with the city, state and federal agencies, including to:
    - protect the lives of the thousands of people that work in the industry;
    - protect the financial assets that have been entrusted for safe keeping and investment;
    - work directly with city and state authorities on emergency coordination and evacuation; and
    - implement the primary objectives in a rapid manner.

  The "lessons learned" from ChicagoFIRST, as reported above and funded by the US Treasury, were published in December 2004, with the hope that additional coalitions will successfully establish similar organizations to strengthen critical infrastructures at a regional level. The Treasury supports the concept of regional coalitions of financial services firms and will work with interested parties to facilitate their formation. For more information, please contact the Office of Critical Infrastructure Protection and Compliance Policy at (202) 622-2602.

Identity Theft Assistance Center (ITAC)

- The Identity Theft Assistance Center (ITAC) was initiated as a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and by enabling law enforcement to identify and prosecute perpetrators of this crime. The ITAC is now officially up and running as the pilot was a success. As of August 2005, more than 2500 victims of identity theft had received assistance from the ITAC. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. The ITAC's services are free-of-

charge to customers and made available based on referrals to the ITAC by one of the ITAC's Members. For additional information, go to www.identitytheftassistance.org.

BITS Product Certification Program (BPCP)

- The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency and National Institutes of Technology and Standards.

Joint Work Plans with Major Software Providers

- BITS' efforts to improve the quality of software security have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them. To facilitate achievement of these objectives, BITS has implemented a joint work plan with one major software provider and is developing joint work plans with others.

SURVEYS AND RESEARCH

Cybersecurity R&D Priorities.

- The results of a 2005 BITS survey on cybersecurity research and development are being used to advise the federal government (Congress, Treasury, the Department of Homeland Security) on its R&D priorities. The BITS survey coincides with the publication of a Cyber Security Industry Alliance (CSIA) paper urging the federal government to play a larger role in coordinating cybersecurity R&D funding. The CSIA paper notes that while the private sector contributes the majority of funds for R&D on cybersecurity, most of this money is for short-term solutions to existing problems. The CSIA and BITS are recommending the federal government organize long-term cybersecurity research to address problems before they emerge.

FOR ADDITIONAL INFORMATION, CONTACT:

Catherine A. Allen, CEO
John Carlson, Senior Director
BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004

(202) 289-4322
cathy@fsround.org
www.bitsinfo.org

ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

Prepared Statement of

Mark Bohannon
General Counsel & Senior Vice President

Software & Information Industry Association (SIIA)

"ICANN and the Whois Database:

Providing Access to Protect Consumers from Phishing"

Before the
Subcommittee on Financial Institutions
And Consumer Credit

U.S. House of Representatives

July 18, 2006

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

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

As the principal trade association of the software and digital information industry,[1] the Software & Information Industry Association (SIIA) has been engaged in the issue of Whois policy for several years, through its active participation in the Coalition for Online Accountability (COA), which consists of many leaders in the copyright industry.[2] COA's goal is to enhance and strengthen online transparency and accountability. It works to ensure that domain name and IP address in the Whois databases[3] remain publicly accessible, accurate, and reliable. In my capacity as General Counsel & SVP Public Policy for SIIA, I actively participate in COA, serve on the Intellectual Property Constituency of ICANN and have seen first hand how the Whois dtabase is a key tool to combat online copyright and trademark infringement, cybersquatting, phishing, and other fraudulent or criminal acts online, including the pernicious effects of spyware.

---

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

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

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

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

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

The Importance of an Accurate, Complete and Accessible Whois

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

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

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

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

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

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

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

---

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

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

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

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

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

Recent Moves to Restrict Access to Whois

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

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

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

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

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

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

---

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

adverse impact on transparency and accountability online.

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

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

The Accuracy and Reliability of Whois Databases Must Improve

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

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

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

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

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

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

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

Conclusion

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

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

Biographical Sketch of

Mark Bohannon

Mark Bohannon is the General Counsel and Senior Vice President Public Policy for the Software & Information Industry Association (SIIA).

As the principal trade association of the software code and information content industry, the more than 750 members of the Software & Information Industry Association (SIIA) develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. Its membership consists of some of the largest and oldest technology enterprises in the world as well as many smaller and newer companies.

Mr. Bohannon is responsible for the legal and public policy agenda of SIIA that includes the areas of taxation, privacy, eCommerce, trade, intellectual property protection, education policy, Internet security, and electronic contracting. Mr. Bohannon's experience includes detailed engagement with hundreds of companies developing online services for the business, consumer and government markets.

Prior to joining SIIA, Mr. Bohannon was a senior official of the U.S. Department of Commerce where he served as Chief Counsel for Technology and Counsellor to the Under Secretary. During his tenure, his responsibilities included a number of technology policy initiatives, and promoting effective eCommerce, intellectual property, and Internet management policies. He was a Vice-Chair of the OECD Working Party on Information Security and Privacy. During his tenure at the Department of Commerce, Mr. Bohannon worked extensively with the National Institute of Standards and Technology (NIST) on a variety of encryption and computer security initiatives for both government agencies and the private sector.

A native of Austin, Texas, Mr. Bohannon is a graduate of the Edmund A. Walsh School of Foreign Service at Georgetown University and of the George Washington University Law School in Washington, D.C.

March 1, 2006

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Before the

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

of the

HOUSE COMMITTEE ON FINANCIAL SERVICES

on

PUBLIC ACCESS TO WHOIS DATABASES

Washington, D.C.

July 18, 2006

I. Introduction

Good morning. Mr. Chairman and members of the Subcommittee, I am Eileen Harrington, a Deputy Director in the Bureau of Consumer Protection at the United States Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to appear before you today to discuss the importance of continued public and law enforcement access to Whois databases. Simply put, the FTC is concerned that attempts to limit the purpose of Whois databases will hinder its ability to protect consumers and their privacy.

As you know, Whois databases are information directories containing contact information about website operators. The FTC has long recognized that Whois databases are critical to the agency's consumer protection mission, to other law enforcement agencies around the world, and to consumers. In fact, four years ago, the Commission testified before Congress on the importance of improving the accuracy of information in Whois databases.[2]

The Internet Corporation for Assigned Names and Numbers, commonly referred to as ICANN, is currently engaged in a policy development process that could modify the information that is maintained on public Whois databases. In April 2006, ICANN's Generic Names Supporting Organization ("GNSO"), the organizational body within ICANN that is evaluating

---

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] Prepared Statement of the Federal Trade Commission on "*The Integrity and Accuracy of the 'Whois' Database,*" Before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, U.S. House of Representatives, May 22, 2002.

the proposed changes to Whois databases, voted to limit the purpose of Whois databases to technical purposes only.[3]

Because of its concern about preserving access to Whois databases, the FTC attended the ICANN meeting in Marrakech, Morocco last month to highlight the importance of public access to Whois databases. On behalf of the FTC, Commissioner Jon Leibowitz participated in a panel comprised of representatives of law enforcement agencies from other countries. He was joined by the Chairman of OPTA, the Independent Post and Telecommunications Authority in the Netherlands that enforces anti-spam laws, and a Deputy Director of Japan's Telecommunications Consumer Policy Division in the Ministry of Internal Affairs and Communications. Collectively, they emphasized the importance of law enforcement access to Whois databases and encouraged the GNSO to reconsider its decision to adopt the narrow purpose definition for Whois databases. The Commission understands that, in part because of these discussions, the GNSO is re-evaluating its decision.

The FTC is pleased to continue this dialogue today by providing this statement on the importance of public Whois databases in enforcing consumer protection laws and in empowering consumers. First, the testimony provides some general background about the FTC. Then, the testimony describes how the FTC uses Whois databases for its law enforcement purposes, discusses the importance of consumer and business access to Whois data about *commercial*

---

[3] The GNSO vote is not final. After considering other recommendations submitted by the Whois Task Force, the GNSO will make formal recommendations to the ICANN Board, which has the ultimate responsibility for making the final decision on any proposed changes to the Whois databases.

websites and other legitimate uses of Whois data, and addresses the privacy concerns that some stakeholders have raised about public access to Whois databases. The statement concludes with some of the FTC's recommendations on how to move forward.

II. FTC Enforcement of Consumer Protection Laws

The FTC is the only federal agency empowered to enforce both competition and consumer protection laws. The principal consumer protection statute that the FTC enforces is the FTC Act, which prohibits "unfair or deceptive acts or practices."[4] The FTC Act authorizes the FTC to stop businesses engaged in such practices. The FTC also can seek monetary redress and other equitable remedies for consumers injured by these illegal practices.

The FTC has used its authority against "unfair or deceptive acts or practices" to take action against a wide variety of Internet-related threats, including Internet auction fraud,[5] Internet-based pyramid schemes,[6] websites making deceptive health claims,[7] and websites promoting "get rich quick" schemes.[8] More recently, the Commission has focused its actions

---

[4] 15 U.S.C. § 45.

[5] *E.g., FTC v. Silverman*, No. 02-8920 (GEL) (S.D.N.Y., filed Aug. 30, 2004).

[6] *E.g., FTC v. Skybiz.com, Inc.*, No. 01-CV-396-AA(M) (N.D. Okla. filed Jan. 28, 2003).

[7] *E.g., FTC v. CSCT, Inc.*, No. 03C 00880 (N.D. Ill., filed Feb. 6, 2003).

[8] *E.g., FTC v. National Vending Consultants, Inc.*, CV-5-05-0160-RCJ-PAL (D. Nev., filed Feb. 7, 2006).

against deceptive claims delivered through spam,[9] "phishing" schemes,[10] and spyware–all violations of consumer privacy that Whois data help us eliminate.[11] In many of these cases, the FTC has worked cooperatively with its consumer protection counterparts across the globe.

In addition, the FTC has made a high priority of protecting consumers' privacy and improving the security of their sensitive personal information, both online and offline. The FTC has brought several law enforcement actions targeting unfair and deceptive practices that involve the failure to protect consumers' personal information.[12] Indeed, the FTC recently created a new Division of Privacy and Identity Protection to address specifically the need to protect consumer privacy and the security of consumers' personal information.

The FTC also promotes consumer welfare in the electronic marketplace through education, outreach, and advocacy. For example, FTC staff provides guidance to businesses

---

[9] *E.g., FTC v. Cleverlink Trading Limited*, No. 05C 2889 (N.D. Ill., filed May 16, 2005).

[10] *E.g., FTC v. _____, a minor*, CV No. 03-5275 (C.D. Cal. filed 2003).

[11] *E.g., FTC v. Enternet Media*, No. CV 05-7777 CAS (C.D. Cal., filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com*, FTC Docket No. C-4147 (Sept. 12, 2005).

[12] *E.g., In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. filed Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005).

advertising and marketing on the Internet[13] and to consumers about what they should look for before making purchases and providing information online.[14]

III. How the FTC Uses Whois Databases

FTC investigators and attorneys have used Whois databases for the past decade in multiple Internet investigations. Whois databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed, it is difficult to overstate the importance of quickly accessible Whois data to FTC investigations.

For example, in the FTC's first spyware case, *FTC v. Seismic Entertainment*, the Commission alleged that the defendants exploited a known vulnerability in the Internet Explorer browser to download spyware to users' computers without their knowledge.[15] The FTC alleged that the defendants' software hijacked consumers' home pages, delivered an incessant stream of pop-up ads, secretly installed additional software programs, and caused computers to slow down severely or crash. The spyware in this case was installed using so-called "drive-by" tactics – exploiting vulnerabilities to install software onto users' computers without any notice. Using Whois data, the FTC found the defendants, stopped their illegal conduct, and obtained a

---

[13] *E.g.*, "Advertising and Marketing on the Internet - Rules of the Road," http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.htm.

[14] *See, e.g.*, "Consumer Guide to E-Payments," "Holiday Shopping? How to be Onguard When You're Online," http://www.ftc.gov/bcp/conline/pubs/alerts/shopalrt.htm, "How Not To Get Hooked By a Phishing Scam," http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm, and OnguardOnline.com (consumer education website providing practical tips concerning online fraud and other online threats).

[15] *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

judgment for millions of dollars in consumer redress.[16] It is uncertain whether the FTC would have been able to locate the defendants without the Whois data.

In another matter, the FTC cracked down on companies that illegally exposed unwitting consumers to graphic sexual content without warning.[17] The Commission charged seven entities with violating federal laws that require warning labels on e-mail containing sexually-explicit content. In these cases, accurate Whois information helped the FTC to identify the operators of websites that were promoted by the illegal spam messages.

Information in Whois databases is most useful when it is accurate. Indeed, the Commission has advocated that stakeholders work to improve the accuracy of such information, because inaccurate data has posed significant obstacles in FTC investigations.[18]

---

[16] *See* News Release, Court Halts Spyware Operations, May 4, 2006, http://www.ftc.gov/opa/2006/05/seismic.htm.

[17] *See* News Release, FTC Cracks Down on Illegal "X-Rated Spam," July 20, 2005, http://www.ftc.gov/opa/2005/07/alrsweep.htm.

[18] Prepared Statement of the Federal Trade Commission on "*The Integrity and Accuracy of the 'Whois' Database,*" before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, U.S. House of Representatives, May 22, 2002 (noting that FTC had found websites registered to "God," "Mickey Mouse," and other obviously false names). FTC investigators have had to spend many additional hours tracking down fraud on the Internet because of inaccurate Whois data – hours that could have been spent pursuing other targets. *See also* U.S. Government Accountability Office, Report to the Subcommittee on Courts, The Internet, and Intellectual Property, House of Representatives, "Internet Management: Prevalence of False Contact Information for Registered Domain Names" (Nov. 2005) (noting that, based on a random sample of domain names from the .com, .net, and .org domains, 8.65 percent of websites were registered with patently false or incomplete data in the required Whois contact information fields).

In some instances, though, even inaccurate Whois information can be useful in tracking down Internet fraud operators. One of the FTC's recent spyware cases involved defendants that used free lyric files, browser upgrades, and ring tones to trick consumers into downloading spyware on their computers.[19] Rather than receiving what they opted to download, consumers instead received spyware with code that tracked their activities on the Internet. In this particular investigation, several of the defendants' websites were registered to a non-existent company located at a non-existent address. Despite the registrant's use of false information, FTC staff was able to link the websites to each other because all of the registrations listed the same phony name as the administrative contact in the Whois databases. Of course, with a "narrow purpose" Whois, not even such inaccurate registration information would be available.

Having "real-time" access to Whois data is particularly important for a civil law enforcement agency like the FTC. Where a registrar is located in a foreign jurisdiction, the FTC often has no other way to obtain the information it needs. The FTC cannot, in most cases, readily require a foreign entity to provide us with information. Thus, particularly in cross-border cases, Whois databases are often the primary source of information available to the FTC about fraudulent domain name registrants.[20]

---

[19] *FTC v. Enternet Media,* No. CV05-7777 CAS (C.D. Cal., filed Nov. 1, 2005).

[20] The number of cross-border complaints received by the FTC continues to rise. In 2005, 20% of the complaints in the FTC's Consumer Sentinel database had a cross-border component, compared to 16% in 2004, and less than 1% in 1995. *See* www.consumer.gov/sentinel.

In short, if ICANN were to restrict the use of Whois data to technical purposes only, it would greatly impair the FTC's ability to identify Internet malefactors quickly – and ultimately stop perpetrators of fraud, spam, and spyware from infecting consumers' computers.

IV. How Consumers Use Whois Databases

Consumers also benefit from access to Whois data for commercial websites. Where a website does not contain contact information, consumers can go to the Whois databases and find out who is operating the website. This helps consumers resolve problems with online merchants directly, without the intervention of law enforcement authorities. Indeed, it is crucial that consumers continue to have the ability to settle disputes prior to–or instead of–law enforcement involvement.

Consumers do in fact regularly rely on Whois databases to identify the entities behind websites. FTC staff recently searched the FTC's database of consumer complaints, and found a significant number of references to the term "Whois." These results indicate that when consumers encounter problems online, the Whois databases are a valuable initial tool they use to identify with whom they are dealing. Consumer access to Whois also helps the FTC because it allows consumers to gather valuable contact information that they can pass on to the FTC – information that might no longer be available by the time the agency initiates an investigation because the website operators have moved on to different scams.

The Organization for Economic Cooperation and Development ("OECD") has recognized that consumer access to Whois data about commercial websites serves an important public policy interest. In 2003, the OECD Committee on Consumer Policy issued a paper unequivocally

stating that "[f]or commercial registrants, all contact data should be accurate and publicly available via WHOIS."[21] In support of this conclusion, the paper says:

> Easy identification of online businesses is a key element for building consumer trust in the electronic marketplace. Because a Web site has no obvious physical presence, consumers are deprived of many of the usual identifying characteristics that help instil trust in a traditional retailer . . . While the most obvious location for an online business to provide contact details is on the Web site itself, domain name registration information can serve as a useful compliment [sic].[22]

This OECD paper represents an international consensus about the importance of accurate and accessible Whois data for consumers.

V. Other Legitimate Uses of Whois Data

There are other legitimate private users of Whois databases–businesses, financial institutions, non-governmental organizations, and intellectual property rights owners–all of which heavily rely on access to accurate Whois data. Although the FTC does not represent these entities' interests in the Whois debate, their use of Whois databases can help consumers. For example, a financial institution concerned about the misuse of its name by "spoofing" its website is not only protecting its own business interests, but it is also protecting its customers from being "phished."

---

[21] OECD, *Consumer Policy Considerations on the Importance of Accurate and Available Whois Data*, DSTI/CP(2003)1/REV1 (April 30, 2003), available at http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-cp(2003)1-final.

[22] *Id.*

The Red Cross recently explained how it used Whois data to shut down fraudulent websites that mimicked its website after Hurricane Katrina in connection with donation scams.[23] The simple yet crucial point is this: many legitimate uses of Whois data by the business community and other non-governmental organizations have an important, and often ignored, consumer protection dimension. Their continued access to Whois information often helps protect consumers from online scams and deception.

VI. Whois Databases and Privacy

Concerns about the privacy of domain name registrants have driven much of the Whois debate. The FTC, as the primary enforcement agency for U.S. consumer privacy and data security laws, is very concerned about protecting consumers' privacy. Thus, the Commission has always recognized that registrants engaged in non-commercial activity may require some privacy protection from *public* access to their contact information, without compromising appropriate real-time access by law enforcement agencies.[24] The FTC supports the further study of how this goal could be achieved. In the meantime, however, at the very least, the FTC believes that ICANN should preserve the status quo and reject limiting the Whois databases to technical uses.

Restricting public access to Whois data for *commercial* websites would deprive the public of the ability to identify and contact the operators of online businesses and would contravene well-settled international principles. If people want to do business with the public, they should

---

[23] *See* Red Cross Comment to GNSO Whois Task Force Preliminary Report, March 14, 2006, http://forum.icann.org/lists/whois-comments/msg00043.html.

[24] *See supra* note 2.

not be able to shield their basic contact information. The 1999 OECD Guidelines on Electronic Commerce state that consumers should have information about commercial websites "sufficient to allow, at a minimum, identification of the business. . . [and] prompt, easy and effective consumer communication with the business."[25] Thus, commercial website operators have no legitimate claim for privacy, and the public should continue to have access to their Whois data.[26]

Moreover, the existing availability of Whois databases can actually help enforcement agencies find out who is violating privacy laws and, consequently, help prevent the misuse of consumers' personal information. For example, Whois databases were invaluable in FTC investigations in phishing cases where the defendants sought to steal sensitive personal and financial information from consumers. In addition, the spyware cases discussed earlier also involve serious threats to consumer privacy, as spyware can monitor consumers' Internet habits and can even retrieve sensitive consumer information, including financial information, by logging keystrokes. Whois data has helped the FTC to stop these privacy violations and, hopefully, will continue to do so.

VII. Recommendations

In light of the FTC's experience in enforcing consumer protection laws, the FTC made several recommendations to the ICANN community at its meeting last month. This testimony

---

[25] OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999), available at http://www.oecd.org/dataoecd/18/13/34023235.pdf.

[26] Consistent with this approach, the European Union's Distance Selling Directive *requires* that European websites ***selling*** to consumers include the name and address of the website operator. European Distance Selling Directive (Directive 97/7/EC), Article 4.

summarizes the recommendations the Commission made to the ICANN community and then concludes with a recommendation that Congress consider enacting the US SAFE WEB Act, which the Senate passed on March 16, 2006.[27]

A. Recommendations to ICANN Community

The FTC made three recommendations to the ICANN community. First, the FTC recommended that the GNSO reconsider and reverse its position that the Whois databases should be used for technical purposes only. If this narrow purpose were to be adopted, the FTC, other law enforcement agencies, consumers, and businesses would not be able to use the Whois databases for their legitimate needs. This would hurt consumers around the world and could allow Internet malefactors to violate consumer privacy with impunity. The Commission understands that the GNSO is currently taking steps to incorporate the input of the FTC and other law enforcement agencies into its final recommendation to the ICANN board.

Second, the FTC encouraged members of ICANN's Governmental Advisory Committee ("GAC") to continue their outreach with law enforcement colleagues in their respective countries to reinforce the serious law enforcement and consumer protection implications of losing access to Whois databases. The Commission is pleased to note that GAC members from several countries are undertaking such an effort.

Third, the FTC recommended that ICANN carefully consider improvements in Whois databases. For example, as the OECD statements referenced above make clear, there is simply

---

[27] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders (US SAFE WEB Act), S. 1608, 109th Cong. (2006) (as passed by Senate, Mar. 16, 2006).

no reason to prevent access to contact information for a commercial website. The FTC urged ICANN to consider additional measures to improve the accuracy and completeness of domain name registration information. The FTC is also interested in exploring the viability of "tiered access" as a solution capable of satisfying privacy, consumer, and law enforcement interests.[28] Restricting the purpose of the Whois databases does not satisfy any of these interests and is a step in the wrong direction. Maintaining accessibility and enhancing the Whois databases would make great strides toward improving the safety and fulfilling the promise of the Internet.

B. US SAFE WEB Act

The FTC has previously recommended that Congress consider enacting the US SAFE WEB Act, passed by the Senate on March 16, 2006. The Commission continues to recommend enactment of this legislation, which would give it additional tools to fight fraud. Even with the current access to Whois databases, the Commission needs these additional tools. If the Commission's access to Whois data becomes unavailable, the Commission's need for the tools provided by the US SAFE WEB Act becomes even more crucial.

The US SAFE WEB Act would make it easier for the FTC to gather information about Internet fraud from sources other than Whois databases. For example, the US SAFE WEB Act would help the FTC obtain information and investigative assistance from foreign law enforcement agencies. It would also allow the FTC to obtain more information from the private sector and from financial institutions about Internet fraud. The FTC's ability to obtain

---

[28] Tiered access refers to a system in which different categories of stakeholders would get different levels of access to Whois databases.

information under the US SAFE WEB Act is no substitute for real-time, desktop access to Whois data. Where such data is limited, inaccurate, unavailable, or inapplicable, however, having access to a broader range of investigative sources about Internet and other cross-border fraud would surely help.

VIII. Conclusion

In sum, the FTC believes that improvements need to be made to the current Whois database system and is committed to working with others toward a solution. In the meantime, ICANN should ensure that Whois databases are kept open, transparent, and accessible so that agencies like the FTC can continue to protect consumers, and consumers can continue to protect themselves. Further, Congress should enact the US SAFE WEB Act to provide the FTC with additional tools to fight Internet and other fraud. Together, these tools will help ensure that consumers are free from deceptive practices that undermine the promise of the Internet.

Testimony of John M. R. Kneuer
Acting Assistant Secretary for Communications and Information
United States Department of Commerce
Before the
Subcommittee on Financial Institutions and Consumer Credit
of the Committee on Financial Services
United States House of Representatives
July 18, 2006

Mr. Chairman,

Thank you and the members of the Committee on Financial Services for inviting me to testify today. I am pleased to have this opportunity to address recent developments related to WHOIS databases, and to share information about the work undertaken by the Department of Commerce in this critical issue area.

The Department of Commerce strongly supports continued, timely access to accurate and publicly available WHOIS data contained in the databases of information identifying registrants of domain names. We believe that WHOIS data is critical to meeting a variety of public policy objectives, including enforcement of laws and consumer protection, and have been pro-actively advocating this position at the meetings of the Internet Corporation for Assigned Names and Numbers (ICANN).

ICANN and WHOIS

The Department of Commerce is committed to preserving the stability and security of the Internet domain name and addressing system (DNS). There exists a Memorandum of Understanding (MOU) between the Department and ICANN, the private sector entity responsible for the day-to-day technical management of the DNS. The MOU contains provisions where ICANN has agreed to continue to assess the operation of WHOIS databases and to implement measures to secure improved accuracy of WHOIS data.[1] In accordance with those specific provisions, ICANN has published three annual reports (as of April 2006) that provide information on community experiences with the InterNIC WHOIS Data Problem Reports system.[2] ICANN has reported that the data collected is being used to ensure that individual registrars are complying with their obligations toward ensuring WHOIS data accuracy.[3] ICANN has also published reports in 2004 and 2005 regarding the implementation of the WHOIS Data Reminder Policy, which requires ICANN-accredited registrars to formally contact domain name registrants on an annual

---

[1] *See* Section II.C.10 of Amendment 6 to the Memorandum of Understanding between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers, available at http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6_09162003.htm.

[2] These reports are available at www.icann.org/whois/wdprs-report-final-31mar04.htm; www.icann.org/whois/wdprs-report-final-31mar05.htm; and www.icann.org/announcements/wdprs-report-final-31mar06.pdf.

[3] All ICANN agreements with generic top level domain name registries and registrars include requirements that domain name registrant contact information be collected, maintained, and publicly posted through WHOIS databases.

basis to review and update their contact information.[4] Again, the underlying purpose of this policy is to improve the accuracy of WHOIS data.

ICANN's Generic Names Supporting Organization (GNSO) has initiated a policy development process, which among other things, seeks to define the purpose of WHOIS data in the following contexts: ICANN's mission and core values; laws protecting individual privacy; laws specifically addressing WHOIS; and the changing nature of registered name holders. In April 2006, the GNSO Council voted in favor of a new definition of the purpose of WHOIS data that is to "resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver." This definition is considered by many, including the U.S. Government, to reflect a narrow, technical definition. The United States public and private sectors are working within the ICANN process to address this problem.

This definition is, however, guiding the subsequent work by the GNSO WHOIS Task Force, which is turning its attention to three specific concerns: 1) determining what data should be available for public access; 2) improving the process for notifying a registrar of inaccurate WHOIS data; and 3) establishing a process for investigating and correcting inaccurate data. When the work of the task force is completed, it will be forwarded to the GNSO Council for review and approval. If approved, it will be forwarded to the ICANN Board for adoption.

The Department's Role and Perspective

I would like to now turn to the work of the Department of Commerce, and specifically to the work of the National Telecommunications and Information Administration (NTIA) regarding this important issue. NTIA serves as the representative for the United States Government to ICANN's Governmental Advisory Committee. Composed of government representatives from over 100 countries, this advisory committee provides advice to the ICANN Board on the activities of ICANN as they relate to the public policy concerns of governments.

ICANN's Governmental Advisory Committee has had several discussions on this topic. In preparation for each advisory committee meeting, NTIA convenes an interagency Working Group that develops and coordinates U.S. positions.[5] Ensuring continued, timely access to accurate WHOIS data is a longstanding, shared priority among all U.S. agencies and has been advocated by the U.S. during these discussions.

As a reflection of that consensus among U.S. agencies, I am very pleased to share with this Committee a formal U.S. statement that was advanced during the June 2006

---

[4] These reports are available at www.icann.org/whois/WDRP-Implementation-30Nov04.pdf, and at www.icann.org/whois/wdrp-survey-report-30nov05.pdf

[5] The Interagency Working Group is comprised of representatives from the Department of Commerce, the Justice Department, the Federal Trade Commission, the State Department, the Patent and Trademark Office, the Federal Bureau of Investigation, the Internal Revenue Service, and the Department of Homeland Security.

Governmental Advisory Committee meeting. The U.S. statement, a copy of which is attached to this testimony, outlines our concerns that a narrow, technical definition of the purpose of WHOIS data would hinder continued access to the WHOIS database for a range of legitimate uses. It could also impede law enforcement's ability to prosecute crimes by allowing perpetrators to hide behind the shield of anonymity. From our perspective, a public WHOIS database is essential to:

- assist civil and criminal law enforcement in resolving cases that involve the use of the Internet; combat intellectual property infringement and theft;
- support Internet network operators responsible for the operation, security and stability of the Internet;
- protect the rights of consumers by facilitating, for example, their identification of legitimate online businesses; and
- assist businesses in investigating fraud, phishing and other law violations.

In developing this consensus position among U.S. government agencies, NTIA has undertaken considerable outreach to and engaged in consultations with a broad range of interested parties, including the financial services sector. In this regard, NTIA facilitated a meeting between U.S. agencies and the companies associated with the Financial Services Roundtable to discuss their concerns regarding the implications of a new, narrow technical definition of the purpose of WHOIS data. We will continue to work with these and other interested parties to ensure that the broad range of legitimate uses of WHOIS data are reflected in the final proposals on WHOIS data that are forwarded by the GNSO Council to the ICANN Board.

NTIA has also actively engaged foreign governments on this issue through ICANN's Governmental Advisory Committee. NTIA serves as the chair of the advisory committee's Working Group on GNSO issues. This working group has identified the public policy aspects of access to WHOIS databases as a priority. NTIA has facilitated information exchanges between the advisory committee and the GNSO to discuss consumer protection and law enforcement perspectives of continued access to accurate WHOIS data. NTIA is working closely with other national governments represented on this committee to develop more formal public policy advice on the purpose and use of WHOIS data.

Finally, I would also note that the ICANN Board passed a Resolution regarding the WHOIS policy process during its June meeting that acknowledges the open dialogue between the Governmental Advisory Committee and the GNSO regarding the issues covered by the WHOIS Task Force terms of reference, as well as the opportunity for public comment from that advisory committee as a whole and from individual member governments. We see this as a positive development that recognizes the important public policy aspects related to access to WHOIS data.

I thank you for this opportunity to update you on this important issue and the progress the Department is making in meeting the needs of U.S. law enforcement and consumer protection agencies. The Department will continue to advocate continued and timely public access to accurate WHOIS data and believes ICANN has provided a productive forum to seek international consensus on WHOIS issues.

Attachment: United States Government Contribution to the Governmental Advisory Committee (GAC) and the Generic Names Supporting Organization (GNSO) on WHOIS

UNITED STATES GOVERNMENT CONTRIBUTION TO THE GOVERNMENTAL ADVISORY COMMITTEE (GAC) AND THE GENERIC NAMES SUPPORTING ORGANIZATION (GNSO) ON WHOIS

The United States Government (USG) would like to officially express its views on the GNSO's WHOIS Task Force report dated March 15, 2006 and the April 12, 2006 vote on the definition of the purpose of WHOIS.

The USG views a public gTLD WHOIS as critical to ensure that international and domestic agencies, businesses and consumers have continued timely and unrestricted access to accurate and complete WHOIS information for the stability and security of the Internet and the international community.

A public gTLD WHOIS is essential to:

- assist each nation's law enforcement agencies, both civil and criminal, in resolving cases that involve the use of the Internet, including child pornography, violent crimes, missing persons, wire fraud, cyber crime, consumer fraud, identity theft, phishing, and other violations of consumer privacy and data security;

- combat intellectual property infringement and theft by being able to identify cybersquatters, trademark infringers and counterfeiters, copyright pirates and other individuals engaged in intellectual property rights violations;

- support Internet network operators that are responsible for the day-to-day operation, security and stability of the Internet;

- protect the rights of consumers by facilitating, for example, their identification of legitimate online businesses; and

- Assist businesses to investigate fraud, phishing, and other law violations that affect their business interests and the interests of their customers.

The USG also recognizes a need to protect the privacy interests of individuals and, like many other nations, protects the privacy of residents of the United States through enforcement of applicable national laws.

Based on the foregoing, the USG believes that Formulation 1 of the Purpose of WHOIS data identified in the *Final Task Force Report on the Purpose of Whois and of the Whois Contacts,* is problematic as it does not reflect the range of public policy interests of a fully functional WHOIS regime.

Specifically, the USG is concerned that Formulation 1, which advances a narrow, technical definition of the purpose of WHOIS, would prevent the range of legitimate uses of Whois databases and impede law enforcement's

ability to prosecute crimes, prevent consumer fraud, and protect consumer privacy by allowing perpetrators to hide behind the shield of anonymity.

The USG will continue to work through the GAC to achieve a consensus and understanding with the GNSO on this very critical issue.

SUZANNE RADELL SENE
GAC Representative -USA
June 2006

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"ICANN and the WHOIS Database:
Providing Access to Protect Consumers from Phishing"

Before the

Subcommittee pm Financial Institutions and Consumer Credit.
Committee on Financial Services
United States House of Representatives

July 18, 2006
2128 Rayburn House Office Building
Washington, DC

I. Introduction

Chairman Bachus, Ranking Member Sanders, and Members of the Committee, thank you for the opportunity to testify today on the WHOIS database and the importance of privacy for the Internet. My name is Marc Rotenberg and I am President and Executive Director of the Electronic Privacy Information Center. EPIC is a non-profit research group founded in 1994 to promote privacy and to focus public attention on emerging civil liberties issues. I am also the former chairman of the Public Interest Registry, which manages the .ORG domain, the third-largest generic Top Level Domain.

EPIC has long been involved in the international discussion of WHOIS policy, as a member of the Non-Commercial Users Constituency within the Internet Corporation for Assigned Names and Numbers (ICANN). EPIC has participated in policymaking decisions with ICANN[1] and has contributed to legal and policy discussions of WHOIS through the publication of the *Privacy and Human Rights* reports[2] and in litigation, contributing an amicus brief detailing WHOIS practices across various country-code top level domains (ccTLDs).[3] Our web page on WHOIS privacy is top-ranked on the Internet.[4]

We very much appreciate the opportunity to appear before the Committee today and to discuss the importance of WHOIS privacy for the Internet. With identity theft the number one crime against consumers in the United States, there is understandable concern about the improper disclosure of personal information on the Internet. The WHOIS database performs a critical function by helping to ensure the security and stability of the Internet. But making the data in WHOIS available to anyone without any accountability creates real risks to the privacy and security of Internet users. We are grateful that the Committee has provided an opportunity to explore these issues in more detail.

II. The Importance of Privacy in WHOIS

To understand the WHOIS privacy issue, it is important to understand the purpose of WHOIS. Because of the distributed nature of the Internet, it is often important to be

---

[1] EPIC & Ruchika Agrawal, Privacy Issues Report: The Creation of A New Task Force is Necessary For an Adequate Resolution of the Privacy Issues Associated With WHOIS (2003), *available at* http://www.epic.org/privacy/whois/privacy_issues_report.pdf; Posting by Marc Rotenberg, Executive Director, EPIC, to mailto:whois-comments@icann.org (Feb. 13, 2006, 16:35:42 EST) (http://forum.icann.org/lists/whois-comments/msg00042.html); Marc Rotenberg, Executive Director, EPIC, to gnso-whoisprivacy-cmts@icann.org (Sep. 30, 2005, 17:08:10 EDT) (http://forum.icann.org/lists/gnso-whoisprivacy-cmts/msg00007.html).

[2] EPIC, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 140 (2005).

[3] Brief *Amicus Curiae* of EPIC in Support of Appellant, *Peterson v. Nat. Telecomm.& Info. Admin.*, No. 06-1216 (4th Cir. Apr. 24, 2006).

[4] EPIC, "WHOIS," http://www.epic.org/privacy/whois/. According to Google for a search on "WHOIS privacy," Jul. 17, 2006.

able to locate a person who is responsible for managing a particular web site or a computer server that is attached to the network. Sometimes, there are technical problems that need to be identified and fixed so that the functionality of the network can be maintained. Other times, there are malicious attacks on computers that require system administrators to contact one another, identify the problem, and develop a solution. Administrators take advantage of the WHOIS directory to find other key technical people and help keep the network running.

ICANN, the non-profit, private-sector corporation that was created to determine technical policy for the Internet, formalized the process of collecting contact information for the WHOIS directory when it required that the "registrars," those are the companies that sell Internet domain names, to collect certain information from "registrants," the people who want to register an Internet domain. Any time that a user wants to register a domain name, she must provide her name, address, email address, and telephone and fax numbers, as well as the name, address, email address, phone and fax numbers of the technical and administrative contact persons. The critical question then becomes how much of this information should be made available to others and under what circumstances.

ICANN, currently requires that all of this information, be available to anyone with an Internet connection. This means that both the law enforcement agent with legal authority to investigate crime and a person with the intent to commit crime has the same access to the WHOIS database. This represents a significant privacy and security risk for a domain name registrant. As EPIC found in our comprehensive review of privacy practices around the world, the ICANN WHOIS data policy has "failed to resolve the privacy risks faced by Internet users that result directly from ICANN's own data practices."[5] Even the widely respected Internet Engineering Task Force acknowledged that there were problems with the growing use of the WHOIS database:

> For historic reasons, WHOIS lacks many of the protocol design attributes, for example internationalization and strong security, that would be expected from any recently-designed IETF protocol....WHOIS lacks mechanisms for access control, integrity, and confidentiality....The absence of such security mechanisms means this protocol would not normally be acceptable to the IETF at the time of this writing.[6]

The lack of security in WHOIS reflected the limited uses that its designers envisioned for it. WHOIS was originally intended to allow network operators to contact those responsible for the technical aspects of another domain, so that technical problems could be resolved.[7] This original purpose is still recognized by the Generic Names

---

[5] PRIVACY AND HUMAN RIGHTS, *supra*, at 143.

[6] Leslie Daigle, Internet Engineering Task Force, *WHOIS Protocol Specification* (2004), http://www.rfc-editor.org/rfc/rfc3912.txt.

[7] Statement of the Registry Constituency, Generic Names Supporting Organization, Preliminary Task Force Report on the Purpose of WHOIS and the WHOIS Contacts, Jan. 18, 2006, http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.htm.

Supporting Organization Council (GNSO), the policy-setting group within ICANN. The GNSO recently recommended that ICANN adopt a formulation for the purpose of WHOIS that maintains this central purpose:

> The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver.[8]

This is an approach that is broadly favored by the registrars, Internet users, privacy experts, and the many government representatives who participate in the ICANN decision-making process. The formulation does not ban non-technical uses for WHOIS data. Instead, it reflects the primary purpose and routine uses for the database. In the smaller academic community in which the Internet first gained ground, there were fewer users and uses, and so fewer threats online. The large amount of contact information and ready access to it were built in to the WHOIS system without considering that the system could be used for a wide range of unanticipated purposes, and that there might be a need to protect the sensitive information in a WHOIS entry, or that there would be non-technical reasons (such as law enforcement) for someone to contact a domain name holder.

The formulation of the purpose of WHOIS therefore represents an attempt on ICANN's part to adjust the WHOIS system to reflect the current state of the Internet and the growing need for user privacy. As the Public Interest Registry, which operates the .ORG top-level domain stated:

> As the Internet and the number of its users has grown, the justification for making WHOIS data publicly available is no longer applicable. While business users may have little or no objection to publication of their contact information, individual users have an expectation of reasonable protection of rights of privacy. They are justifiably concerned that far more information is now publicly available than is necessary for any legitimate purpose.[9]

ICANN, in developing the current policy for WHOIS, is primarily concerned with ensuring that the database is accessible to network administrators and providing a reasonable amount of privacy protection for Internet users. But ICANN does not restrict law enforcement access to WHOIS data. At a recent meeting in Marrakech, Paul Twomey, the president and CEO of ICANN, clearly stated that the purpose of the

---

[8] Generic Names Supporting Organization Council, ICANN, "GNSO Council Motions 12 April 2006," http://gnso.icann.org/mailing-lists/archives/council/msg02393.html.

[9] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.

WHOIS formulation is not to bar law enforcement access. Twomey said, "I cannot see a circumstance where law enforcement agencies will not have access to this information."[10]

Many groups involved in the debate over domain name policy agree on this approach. The Non-Commercial Users Constituency,[11] which represents a wide range of non-commercial domain name holders, highlighted this point in its comments on the WHOIS purpose formulation. After noting that WHOIS was not created with the intention of serving litigants or law enforcement, the group stated:

> Companies with allegations against domain name registrants can seek subpoenas of specific subscriber records through Internet service providers, or learn about a domain name registrant's identity information through requested subpoenas of registrar records.
> ...
> Law enforcement agencies can subpoena specific subscriber records through Internet service providers, or learn about a domain name registrant's identity information through subpoenas of registrar records.[12]

The Public Interest Registry also indicated that the purposes of WHOIS are best served by limiting unrestricted and unaccountable access to the database, while still allowing for law enforcement access under appropriate circumstances:

> As a general rule, information available in response to public, anonymous inquiries (whether from registries or registrars) should be limited to domain names, the identity of the registrar and an email address to contact the registrar....[L]aw enforcement agencies with an appropriate legal basis for a request, e.g., a subpoena, should be able to have access to personal information when necessary for law enforcement purposes.[13]

Establishing clear privacy safeguards for the WHOIS database, as ICANN intends to do, is also necessary to reconcile the collection of personal information that ICANN requires for those who register Internet domains with the laws of many countries that explicitly protect the WHOIS data. Peter Schaar, chairman of the leading group of European privacy officials (the Article 29 Working party), recently wrote to the ICANN board of directors, pointing out that, under European privacy law,[14] any data collected and processed must be relevant and not excessive for the purpose for which it was

---

[10] Thomas O'Toole, *ICANN Official Says Government Worries About Loss of Whois Access Are Unfounded*, 11 BNA ELECTRONIC COMMERCE AND LAW REPORT 762, Jul. 12, 2006.
[11] EPIC is a member of the Non-Commercial Users Constituency.
[12] Non-Commercial Users Constituency, *NCUC constituency statement on Whois purpose*, Aug. 9, 2005, http://www.ncdnhc.org/policydocuments/ncuc-whois-purpose-9-Aug-05.pdf
[13] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.
[14] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

collected.[15] In the case of WHOIS, collecting and publishing all registrants' contact information and addresses far exceeds the disclosure necessary to resolve technical problems. Even law enforcement purposes can be easily served by a narrower disclosure.[16]

These proposals represent a sensible step towards protecting the sensitive information of domain name holders, protecting a reasonable expectation of privacy in personal information in everyday transactions.

B. Privacy Threats Raised by Unrestricted Disclosure of WHOIS Data

Protecting registrants' addresses, email addresses, and telephone numbers from inappropriate use is a real problem. The personal information available in the WHOIS database can be used for phishing, spamming, stalking, and the suppression of free speech. The problem of identity theft is particularly serious in the United States. According to the Federal Trade Commission, complaints about identity theft topped the list of consumer complaints last year, accounting for 255,000 of more than 686,000 complaints filed with the agency in 2005.[17]

This risk of identity theft combined with the lack of privacy for WHOIS data could affect millions. In the third quarter of 2005 alone, 8.5 million new domain names were registered, bringing the total number of domain names to a record-setting 86.5 million.[18] Registrants include not only large and small businesses, but also individuals, media organizations, non-profit groups, public interest organizations, support groups, and political and religious organizations.[19] ICANN currently requires all of these companies, organizations, and individuals to provide contact information for the WHOIS database. Understandably, there is growing concern about the possible misuse of the data.

Such a massive database of contact information is a treasure trove for spammers and phishers. In 2005, the most prolific spammer in the United Kingdom was found liable for harvesting email addresses from the WHOIS database to use in spam mailings that defrauded domain name holders into giving up financial information.[20] Armed with the personal information of Internet users the phisher was able to pose as a registrar, asking users to renew registrations for a fee. Other fraudsters may use the data to impersonate

---

[15] Letter of Peter Schaar, Chairman of the European Commission's Article 29 Working Group, to Vinton Cerf, Chairman of the Board of Directors, ICANN, Jun. 22, 2006, *available at* http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf

[16] Schaar's letter continues by describing a layered approach that would be more proportionate, where "details of the person are known to the ISP that can, in case of problems related to the site, contact the individual or transmit the information to an enforcement authority entitled by law to access this information." *Id.*

[17] Federal Trade Commission, "FTC Releases Top 10 Consumer Fraud Complaint Categories: Identity Theft Again Leads the List," (Jan. 25. 2006), http://www.ftc.gov/opa/2006/01/topten.htm.

[18] VeriSign Domain Name Industry Brief, "The VeriSign Domain Report," November 2005, http://www.verisign.com/static/036316.pdf.

[19] *See* PRIVACY AND HUMAN RIGHTS, *supra*, at 140.

[20] Dinah Greek, *Weasel out of this one*, COMPUTERACTIVE, Feb. 11, 2005, *available at* http://www.vnunet.com/computeractive/news/2012383/weasel.

the domain name registrant to other entities, such as phone companies, retailers, or even financial institutions, gaining access to even more sensitive information.

Even more sinister threats are easy to envision. Individual domain name registrants may have no address to provide other than their home address, and no phone number other than their home or mobile phones. The ready availability of this information on WHOIS puts at risk for stalking or other criminal activity anyone who chooses to register her own domain name. In some situations, a person who would register an Internet web site and provide a useful service to others may choose not to simply because of the lack of privacy safeguards.

Protecting free speech on the Internet also requires protecting the privacy of WHOIS data. A user speaking from his own website, or sending an email from his own domain, currently must surrender his right to speak anonymously. An anonymous speaker in this country, for instance, might find his residence or his telephone numbers subject to harassment for voicing unpopular opinions. In other countries, Internet dissidents face the persecution of oppressive regimes.[21] Someone expressing opinions counter to those of the government may be refused space on local commercial hosts, or may suspect that those hosts would turn his contact information over to authorities.[22]

Already governments are trying to crackdown on human rights groups by extending identification requirements for Internet users.[23] Requiring that a dissident publish his Internet contact information for ready access by government threatens democratic reforms in several countries.[24] The United States should not be on the wrong side of this important twenty-first century human rights issue by opposing privacy safeguards for the WHOIS database.

C. Current Methods Used to Protect Privacy

---

[21] *See generally* REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom*, http://www.rsf.org/rubrique.php3?id_rubrique=578 (detailing the arrests, imprisonment, harassment, or torture of Internet speakers in several countries around the world).

[22] Xiao Qiang, *Yahoo helped sentence another cyber dissident up to 8 years - Liu Xiaobo*, CHINA DIGITAL TIMES, Feb. 8, 2006, http://chinadigitaltimes.net/2006/02/yahoo_helped_sentence_another_cyber_dissident_to_8_year_1.php; Hiawatha Bray, *US to Protest Censorship of Internet by Beijing*, BOSTON GLOBE, Feb. 15, 2006 at F1 (noting Yahoo's complicity in identifying two Chinese Internet dissidents); BBC NEWS, *Yahoo "helped jail China writer"*, Sep. 7, 2005, *at* http://news.bbc.co.uk/2/hi/asia-pacific/4221538.stm; Richard Spencer, *Microsoft pulls plug on China protest blog*, THE DAILY TELEGRAPH, Jan. 6, 2005, at 18.

[23] Maria Sanminiatelli, *Italian Law Hits Cybercafes*, SAN JOSE MERCURY-NEWS, Dec. 12, 2005, at 4E; REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom* (noting identification requirements or special permissions required in Bahrain, Cuba, Syria, and Turkmenistan).

[24] REPORTERS WITHOUT BORDERS, *2006 Annual Report on Internet Freedom* (harassment and censorship of opposition websites in Belarus; arrest of a blogger in Egypt; censorship and arrests of bloggers in Iran; censorship and arrests in Lybia; government intimidation of journalists and bloggers in Malaysia; imprisonment and torture of Internet users in Syria; silencing of critical websites in Thailand; censorship and jailing of dissidents in Tunisia; jailing of dissidents in Vietnam).

Since ICANN makes that the WHOIS data available without any legal process to protect personal information from improper use, domain name registrants have understandably taken steps to protect their personal privacy and security. One such method is simply to enter inaccurate information. This is not surprising. Women, for instance, have often provided just an initial, rather than a complete first name, in the phonebook to protect privacy. Similarly, legitimate Internet users, knowing that others may obtain their address and phone number, will simply enter false data into the system. Here, we can see how the lack of privacy protection undermines the desire for accuracy.

Other users take advantage of a proxy service, either offered by a registrar or a third party, that helps shield the identity of the registrant. These services provide their own contact information for the WHOIS database, passing along any contact or communications to the registrant. In this way, the original purpose of the WHOIS database can be achieved, since messages sent to resolve any problems with the website will still reach the registrant, while preventing the registrant's personal information from being improperly disclosed.

Unfortunately, some registries, such as the United States' country code top-level domain, .US, forbid the use of proxy registration. Such policies further expose registrants under these domains to risk of harm and encourage inaccurate data entry, though fortunately they appear to be the exception to the rule.[25] Still, we believe the current policy of the Department of Commerce for .US is poorly conceived and should be revised.

III. A Model for a Sensible, Effective WHOIS Service

Both of the methods currently available for registrants to protect their data, however, are incomplete solutions. For one, users should not be required to lie to protect their privacy. Furthermore, some users may be unable to afford a proxy registration service, or the service may be banned in their countries. Also, as the Public Interest Registry has pointed out, the Registrar Accreditation Agreement requires proxy providers will be liable for users' actions.[26] Because of this, many users may not be able to use proxy services, if their views are too controversial for proxy providers. This may be a particular problem in countries that do not protect fundamental human rights.

A sensible privacy solution would simply remove the most sensitive data from being viewed by any member of the public. Such solutions have been proposed by registries,[27] registrars,[28] non-commercial users,[29] and others.[30] These proposals would

---

[25] Brief *Amicus Curiae* of EPIC, *Peterson v. Nat. Telecomm. & Info. Admin.*, No. 06-1216 (4th Cir. Apr. 24, 2006).

[26] Comments of the Public Interest Registry on the Final Report on WHOIS Accuracy and Bulk Access, WHOIS Task Force, Generic Names Supporting Organization, Feb. 17, 2003, http://pir.org/PDFs/pdf00000.pdf

[27] Public Interest Registry, Policy Statement Regarding the WHOIS Service, Mar. 2, 2005, http://pir.org/PDFs/pdf00000.pdf.

[28] Paul Stahura et al. Proposal to Increase Whois Utility and Relevancy: The Operation Point of Contact, Nov. 22, 2005, *available at*

allow the WHOIS database to comply with Fair Information Practices, which require that individuals know, when they disclose personal information about themselves, how that data will be used and who will be able to view it.

Currently, those accessing the Whois database lack these safeguards. This type of disclosure not only violates principles of good information practice and data security, it potentially runs afoul of international laws such as the European data protection directive. As Chairman Schaar pointed out in his letter, the widespread availability of WHOIS data is not proportionate to the problems the database is meant to solve.

An important distinction can also be drawn between corporate domain name holders and individuals. As with telephone listings, the motivations behind publicizing commercial, or private, contact information differ. As a business that holds itself out to the public and must be accountable for its business dealings, a corporation can reasonably be expected to publish contact information at which it can be reached for questions, complaints, and service of process. Individuals, however, will often use their domains as they would a personal means of communication—such as a cell phone, the number to which they have no public duty to disclose.

But a comprehensive approach to WHOIS cannot rely solely on the distinction between commercial and non-commercial registrants. There should be some point of contact for all who register an Internet site, and there should be clear safeguards to protect personal information from improper disclosure. Under a proposal now being pursued by ICANN – the oPOC or "Operational Point of Contact" – domain name registrants will still provide their name, address, phone, and email contact information when they register, but personal privacy will be protected, since only the operational contact's information will be published.[31]

Large businesses could certainly list themselves, while smaller organizations and individuals would probably list their registrar or ISP – the organizations best equipped to respond to technical problems. Under this arrangement, there would be no change in the collection of registrant data; Individuals and businesses who register Internet sites would still be required to provide contact information that will be accessible to law enforcement and others, subject to due process safeguards.

---

http://code.byte.org/_attachments/1426464/Proposal%20to%20Implement%20oPOC%20-%2011282005.pdf

[29] Non-Commercial Users Constituency, *NCUC constituency statement on Whois purpose*, Aug. 9, 2005, http://www.ncdnhc.org/policydocuments/ncuc-whois-purpose-9-Aug-05.pdf

[30] Letter of Peter Schaar, Chairman of the European Commission's Article 29 Working Group, to Vinton Cerf, Chairman of the Board of Directors, ICANN, Jun. 22, 2006, *available at* http://www.icann.org/correspondence/schaar-to-cerf-22jun06.pdf

[31] "Proposal to Increase Whois Utility and Relevancy: The Operational Point of Contact, Rationalizing the gTLD Whois System and Specific Contact Records,"http://www.dnspolicy.org:4080/index.php?n=Main.OperationalPointOfContact; *original available at* http://code.byte.org/_attachments/1426464/Proposal%20to%20Implement%20oPOC%20-%2011282005.pdf.

An effective model for WHOIS privacy would therefore take into account the limited amount of information necessary to accomplish the technical goals of the database; recognize that law enforcement needs for data should not require widespread disclosure of personal information; and provide a process for releasing, in certain well-defined circumstances, data that is not routinely made available.

That is the approach that ICANN is now pursuing. It is backed by the key stakeholders and the user community. It is a sensible and effective solution that should be supported.

IV. Privacy is Compatible with, and Enhances Accuracy and Accountability

As many have recognized, there are legitimate uses for WHOIS data. If a network administrator notices problems with a connection to another network, for example, he can use the WHOIS information to contact someone at the other network who will be able to resolve the problem. The WHOIS database is a useful tool for network administrators to resolve problems with interconnected networks.

The need for accurate WHOIS information, though, does not mean that privacy must be sacrificed: there is a limited amount of information that needs to be made available, and there are limited classes of people who need access to that information. In most cases, the persons using WHOIS need only a reliable method of contacting the responsible party. That contact information does not need to include all, or even any, of the personal information about the domain name registrant, and it does not even need to be personally identifiable. A registrar or third party proxy can easily pass on communications to the domain name holder without revealing private information to the Internet at large.[32] Where direct contact is necessary, an email address or Post Office Box can suffice. Most of all, though, none of this information needs to be publicly available to anyone on the Internet. Restricting access to network administrators achieves the goals of WHOIS while helping protect the privacy of registrants. The types of information needed and the types of people who need it can be and should be itemized and limited.

In fact, limiting the information made available and the people who can access it promotes the accuracy and therefore the usefulness of the information. One reason users provide false WHOIS information is that they know it will be publicly available for spammers, stalkers, and anyone else on the Internet who wants it. If users know that their information will only be made available to people who actually need it, and that those people will only be getting the information they need, this incentive to provide false information evaporates. The need for accuracy and truthfulness is what underlies the importance we place in doctor-patient confidentiality or attorney-client privilege. When information is protected by medical confidentiality, attorney-client privilege, shield laws, or tighter WHOIS privacy policies, people place themselves at less risk when giving out personal information and are more likely to provide accurate information.

---

[32] Carl Bialik, *New Services Are Making It Easier to Hide Who Is Behind Web Sites*, Wall Street Journal, Sept. 30, 2004, at A1.

V. Unrestricted Access to WHOIS is an Ineffective Approach to the Phishing Problem

Phishing involves three steps: setting up a web site to collect information, getting people to go to the site (usually via spam), and collecting the information. A phisher sets up a web site generally by copying the design of a login page for a bank or other trusted web site. This page is then set up on a free or fraudulently obtained web site, a hacked web site, or a hacked personal computer. Once it is operational, the phisher sends out emails that appear to be official notices asking users to visit the site and enter their financial information. When the information is submitted, the phisher stores it and uses it to commit fraud or theft. In some cases, phishers have even set up the site to check the validity of the information and prompt the user if it is not correct.[33]

There are many victims of this kind of fraud in addition to the person whose financial information is used. A computer is hacked to host the web site, or someone else's financial information is used to fraudulently pay for hosting, and hacked computers are often used to send out the spam messages luring users to the site. Because of this setup, the identity of the actual phisher, who is often even outside of the United States, is hidden. Instead, only the hosting and spamming computers are known.

Once a hosting web site has been identified, WHOIS may be useful in shutting the site down. Because the phishing sites are usually short-lived, the spam announcements generally refer to them by IP address rather than domain name, so the WHOIS IP database is used to find the administrator for the network. That is, WHOIS is used as a technical means of finding the person who controls the hosting computer's network access. In many cases, the WHOIS database of domain name registrants is not even used.

However, in finding the perpetrator himself, the WHOIS database may be less useful. Since the computers used to send the spam or host the fraudulent website are often hacked, or the domain names registered under stolen account information, the results of a simple WHOIS search will not lead law enforcement to the fraudster.

In fact, open access to the WHOIS database may contribute to phishing and spam. Phishers and spammers must build a list of email addresses to which they can send their messages, and the WHOIS database contains an email address for the owner of every domain name. Spammers can "harvest" this database to quickly build a list of recipient addresses. Because spam's success depends on the miniscule cost of sending each message, bulk "harvesting" of email addresses from WHOIS can be hindered by even a moderately successful method of limiting access to domain registrants' information to people who have legitimate needs for it. In addition, as described above, users will be more willing to give accurate contact information when they know it will not be used by spammers and phishers.

---

[33] Brian Krebs, *Citibank Phish Spoofs 2-Factor Authentication*, Jul. 10, 2006, http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html (last visited July 14, 2006).

VI. Conclusion

The public availability of WHOIS information has resulted in harassment and criminal acts, some of which the Committee today is working to prevent. Rather than mandating more disclosure of this information, though, the Committee should both protect domain name holders' privacy and increase the usefulness of information in the WHOIS database by limiting access. When registrants feel that their personal information will remain safe and will only be used for legitimate purposes, they will be more willing to provide accurate information. As long as the personal information is published and available for anyone on the Internet, including spammers, stalkers, hackers, and phishers, registrants will be hesitant to give correct information. A private, accurate database is no less useful for resolving technical problems and for legal investigations than the current database, but it would protect the privacy of millions of domain name holders.

ICANN has made significant progress addressing the twin concerns of online fraud and privacy protection. The WHOIS proposal currently under consideration will still permit law enforcement access to WHOIS data under appropriate circumstances, but will limit the possibility that personal information will be improperly disclosed to spammers, phishers, stalkers, and governments intent on stopping democratic reform.

We appreciate the Committee's interest in this important issue and hope that Members agree that privacy protection remains a central concern for Internet users and the future of Internet-based services.

AIPLA
AMERICAN INTELLECTUAL PROPERTY LAW ASSOCIATION
2001 JEFFERSON DAVIS HIGHWAY • SUITE 203 • ARLINGTON, Virginia 22202

June 15, 2006

Comments of the American Intellectual Property Law Association regarding the GNSO Council vote in favor of the Formulation 1 definition of the purpose of the WHOIS service

The American Intellectual Property Law Association (AIPLA) wishes to express its serious concerns regarding the vote of the Generic Names Supporting Organization (GNSO) favoring a narrow definition of the purpose of the WHOIS service in the context of ICANN's mission and core values.

AIPLA's 16,000 members are primarily lawyers in private and corporate practice, in government service, and in the academic community comprising a wide and diverse spectrum of individuals involved in the practice of patent, trademark, copyright, trade secret and unfair competition law. AIPLA members represent both owners and users of intellectual property, including many large and small businesses that make commercial use of Internet websites or otherwise provide services over the Internet.

In 2003, ICANN appointed a Taskforce to report on the purpose of WHOIS and WHOIS contacts. When the Taskforce was unable to reach consensus on a single definition of WHOIS, public comments were solicited from stakeholders on two Formulations:

Formulation 1:

"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver."

Formulation 2:

"The purpose of the WHOIS service is to provide information sufficient to contact a responsible party or parties for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, technical, legal or other issues related to the registration or use of a domain name."

Responses were received from a total of 38 individuals and organizations. Of those respondents, eight individuals favored Formulation 1, whereas 30 companies, organizations, and individuals favored Formulation 2. Those preferring Formulation 2 included organizations such as Sony Pictures Digital, eBay, Mars UK Limited, INTA, AIPLA, and AMMPI, as well as the Dutch, Serbian, and Austrian anti-piracy coalitions.

Notwithstanding the broad support for Formulation 2, on April 12, 2006, the GNSO voted in favor of Formulation 1 which, if ultimately adopted by ICANN, would render it exceedingly difficult for law enforcement, intellectual property owners, and financial institutions to access necessary contact information about domain name holders.

There are many reasons why the broader Formulation 2 definition of WHOIS is preferable:

1. A pattern of behavior that can lead to an inference of bad faith which, under the UDRP, can result in the transfer of a domain name from a bad faith registrant is frequently only provable through WHOIS;
2. Unchecked IP infringement undermines business viability and technical stability and could result in Internet fragmentation;
3. Accurate and available information is essential for law enforcement in crimes including spamming, denial of service attacks, identity theft and account fraud, hate literature, terrorism and child pornography;
4. The requirement to provide accurate contact and identity information acts as a deterrent to trademark infringement, copyright infringement, cybersquatting, phishing, typosquatting and other IP cyber infringements and facilitates enforcement of IP rights.

For these reasons, AIPLA respectfully requests that:

- the GNSO Council members from the Noncommercial Users Constituency, the Registrar Constituency, and the Registry Constituency reconsider their positions favoring a narrow definition of the purpose of WHOIS and adopt a definition meeting the needs of all Internet users;
- the Government Advisory Committee, in recognition of the adverse impact that a narrow definition of the purpose of WHOIS would have on the viability and technical stability of the Internet, urge the GNSO to adopt a definition meeting the needs of all Internet users; and,
- the ICANN Board closely monitor the policy development process and bear in mind the importance of preserving the existing requirements to make up-to-date and accurate WHOIS information available to all who have a legitimate need to obtain such information.

Statement Submitted by

Lynn Goodendorf
Vice President Information Privacy Protection
InterContinental Hotels Group

to the
House Financial Services Subcommittee on
Financial Institutions and Consumer Credit

July 18, 2006

I am pleased to have this opportunity to submit this statement to the House Financial Services Subcommittee on Financial Institutions and Consumer Credit on behalf of InterContinetal Hotels Group (IHG). IHG is the world's largest hotel company, and companies in IHG own, manage and franchise several of the world's most famous global hotel brands, including InterContinental, Holiday Inn, Holiday Inn Express, Crowne Plaza, Staybridge Suites, Candlewood Suites and Hotel Indigo. IHG owns, manages, leases or franchises, through various subsidiaries, over 3,600 hotels and 537,500 guest rooms in nearly 100 countries and territories around the world.

Mr. Chairman, your holding of this hearing on "ICANN (Internet Corporation for Assigned Names and Numbers) and the Whois Database: Providing Access to Protect Consumers from Phishing" is both timely and important.

For InterContinental Hotels Group, e-commerce is a strategic sales channel for growth and profits. Our customers booked more than $1 billion on our websites last year, and www.holiday-inn.com was the most frequently visited hotel brand site in the world. We need to reassure consumers in their use of e-commerce and encourage consumer confidence that businesses will use and protect information in a responsible manner.

Our company is concerned with reports such as a recent Unisys survey showing that 73% of Americans are worried about thieves using their bank account or credit cards. And we are troubled by a recent Consumer Report "WebWatch" indicating that 30% of adult Internet users say they have reduced their overall use of the Internet, with another 25% saying they have stopped buying things online.

That is why we as a company, and I as a privacy and security professional, are seriously concerned about the resolution adopted on April 12 by ICANN's Generic Names Supporting Organization (GNSO) Council to define the "purpose of Whois" as only to

"resolve issues related to the configuration of records associated with the domain name within a DNS nameserver."

Those of us in the travel and hospitality industries depend on ready access to Whois data to enhance accountability and transparency online, and we believe such a policy change will have a seriously detrimental effect on our consumer protection efforts both in the U.S. and abroad.

Travel and hospitality companies use Whois in several ways: 1) to identify parties responsible for registration of misleading domain names, which are often the source of online frauds, phishing schemes and other practices that cause consumer confusion; 2) to prevent or investigate misconduct facilitated by misleading registrations; 3) to cooperate with law enforcement to protect consumers in cases of fraudulent websites and e-mails; and 4) to protect our legitimate intellectual property rights.

If the "purpose of Whois" is defined narrowly as proposed by GNSO, most of the data now in Whois could be cut off from public access – including data as fundamental as the name of the domain name registrant. If the change were to be implemented in new ICANN rules, most of the current public and business uses of Whois would become virtually impossible.

Consumer protection is the primary concern in Internet commerce. Our businesses need access to the Whois database to protect the privacy and security of our customers and to reduce the risk of online fraud, including identity theft. Internet users would lose significant privacy protections under the narrowly defined "purpose of Whois." For example, cases of fraud or trademark infringement might not be considered "technical issues." Since time is of the essence in addressing these cases, we must be able to respond as quickly as possible by having immediate and unrestricted access to the Whois database.

To protect our hotel consumers, we use Whois repeatedly on a daily basis to identify domain name registrants and website operators that are creating websites and sending e-mails using our trademarks to mislead consumers. Given the large number of hotel consumers we serve and the well-known brands we represent, including Holiday Inn and InterContinental, our hotel consumers and our companies are prime targets for cybersquatters, phishers, spammers and other bad actors on the Internet.

To help shield our hotel consumers from such illegal activities on the Internet, we file complaints under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP") to obtain the transfer of domain names that are being used by others in bad faith. For example, to protect hotel consumers from viewing a pornographic website using its famous Holiday Inn trademark in a domain name, Six Continents Hotels, Inc. (an InterContinental Hotels Group company), recently obtained the transfer of the domain name <holidayinnmanassas.com>. *Six Continents Hotels, Inc. v. CredoNIC.com / Domain For Sale*, WIPO Case No. D2005-0755. We have also obtained the transfer of numerous other domain names through the UDRP process and in other ccTLDs.

We also regularly use Whois to contact domain name registrants and successfully negotiate the voluntary transfer of problematic domain names without incurring the time and expense of the UDRP process. Further, we use Whois for other legal purposes, such as to identify copyright infringers who are violating our companies' legal rights.

Mr. Chairman, without the benefit of unrestricted access to a database of information about, and contact information for, domain name registrants, we would find it difficult, if not impossible, to protect the public and enforce our rights on the Internet as we currently do. Any effort to reduce the amount of information in the Whois database or to limit our access to it would undermine our ability to assert our legal rights.

Consequently, our consumers would be harmed by, for example, being led to pornographic and inappropriate websites. Furthermore, our consumers might be forced to bear the burden of the increased financial expenses we would have to incur to identify website operators through court proceedings and private investigations if the Whois database or access to it were modified.

At the very least, we believe that accessibility to the existing types of information in the Whois database should remain as-is. Although I must point out that we also have serious doubts about the existing accuracy and reliability of this database and its abuse by domain name registrants. For example, in one UDRP case filed and won by InterContinental Hotels Group's Six Continents Hotels, Inc., the registrant was listed in Whois as, literally, "Sdf fdgg" – an obvious random typing of characters on a computer keyboard. The domain name was being used in connection with a website that automatically redirected users to a site that contained pornographic images of partially clothed people urinating, and links to other pages, including those labeled "Rape Site" and "Incest & Mature Site." *Six Continents Hotels, Inc. v. Sdf fdgg*, WIPO Case No. D2004-0384.

Finally, let me mention that we have heard concerns that publicly available information in the Whois database should be limited to safeguard the privacy of domain name registrants. However, existing systems already exist for this purpose, through the so-called "domain proxy" or "domain privacy" services offered by many registrars that mask the true identify of their registrants while cooperating with intellectual property owners and law enforcement personnel. Therefore, no change to the Whois system is necessary to safeguard the privacy of domain name registrants, since such a system already exists.

Mr. Chairman, it is critical that ICANN preserve and enhance access to Whois data for purposes of protecting consumers and fighting fraud. We hope, too, that ICANN will work to further enhance the accuracy of the Whois database. There is a tremendous public interest value in a rich Whois data set with information on registrants and administrative contacts. The current long-standing rules on access to Whois are the best way to fulfill this important consumer protection need and they should, at least, be maintained, if not improved.

Thank you for your leadership on this important issue, Mr. Chairman. Your early and strong interest in the Whois issue is a vital part of the consumer protection and anti-identity theft efforts you have championed in the Congress. We thank you for this opportunity to express our concerns, and we would be happy to assist you in every way possible to address these issues.

NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS
3138 10th Street N. • Arlington, VA • 22201-2149
(703) 522-4770 • (800) 336-4644 • FAX (703) 522-2734

FRED R. BECKER, JR.
President and CEO

July 17, 2006

The Honorable Spencer Bachus
Chairman
Subcommittee on Financial Institutions & Consumer Credit
House Committee on Financial Services
Washington, DC 20515

Dear Chairman Bachus:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association that exclusively represents the interests of our nation's federal credit unions, we are writing to commend your leadership in protecting consumers and for holding the July 18th hearing: "ICANN and the Whois Database: Providing Access to Protecting Consumers from Phishing." We believe the time is right for Congressional oversight on this important topic.

Our nation's federal credit unions are working hard to educate their members about "phishing" scams, as unfortunately the criminals that originate these scams have targeted a number of credit unions and their members. Even the National Credit Union Administration (NCUA) has been a target of these scams. They have responded by putting a warning about the scams on their homepage.

Only a few months ago, NAFCU was targeted as part of a "phishing" scam. Fraudulent e-mails that appeared to be from NAFCU were sent as spammed mail to lure unsuspecting victims to divulge personal information such as credit card numbers, bank account information, and Social Security numbers. Unfortunately, NAFCU's name, logo and other graphics were used to manipulate people into providing such information on several occasions. In response, we have made alerting our members and the public a priority via our Member Service Center and Web site on how to avoid being made a victim.

Further, NAFCU has reported this "phishing" e-mail activity to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center in addition to the National White Collar Crime Center. As on-line banking, shopping, and business transactions increase, NAFCU believes that financial education must now include arming consumers with protecting oneself against potential fraud and identity theft, particularly over the Internet.

NAFCU is pleased that the Subcommittee recognizes the urgency and importance in protecting our nation's consumers and the over 89 million credit union members. Please do not hesitate to contact me or Brad Thaler, NAFCU's Director of Legislative Affairs, for more information.

Sincerely,

Fred R. Becker, Jr.
President/CEO

cc: The Honorable Bernie Sanders
House Financial Institutions and Consumer Credit Subcommittee

BITS
FINANCIAL SERVICES
ROUNDTABLE

1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

April 14, 2006

To: Internet Corporation for Assigned Names and Numbers

e-mail address: <whois-comments@icann.org>

Re: WHOIS Data Base

Dear Sirs and Madams:

The purpose of this letter is to comment on the proposal before the Internet Corporation for Assigned Names and Numbers (ICANN) to limit the type of information collected and maintained in the WHOIS data base. Based on a review of the information provided in the January 18, 2006 task force report containing two opposing formulations of the "purpose of WHOIS," and discussions among information security and fraud risk managers, we urge ICANN to adopt Formulation 2.[1] Formulation 2 will provide financial institutions with the information they need to respond to identity theft and account fraud. In addition to commenting on the two proposals, we want to outline the activities of BITS and our members in addressing information security and identity theft challenges.

Under formulation 1, the only purpose of WHOIS is to "resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver" (i.e., narrow technical issues). Under formulation 2, the purpose of WHOIS is to help resolve a broader range of "technical, legal or other issues regarding registration or use of a domain name." We believe the adoption of formulation 1 would make it more difficult and time-consuming for financial institutions to identify and stop domain-based scams and the identity theft and account fraud that result.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. Further, financial institutions must also deal with other domain-based issues including, but certainly not limited to, trademark infringement, unauthorized and sometimes unlawful disclosure of confidential, proprietary or customer information, spam attacks, inappropriate content sent or received via email, staff harassment/stalking, and violation of intellectual property rights by web site operators. While our members' foremost concern is to protect their customers and maintain their trust, they must also be mindful of the need to comply with the requirements set forth by numerous laws, regulations and supervisory guidance.

---

[1] http://www.icann.org/announcements/announcement-18jan06.htm)

We believe that formulation 1 (or other efforts to limit or narrow the information) in WHOIS could adversely affect the financial services industry's efforts to respond identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Often times, the fraudsters will register a domain name in the name of innocent consumers without the knowledge of the consumer. In most instances, it is not until these unsuspecting consumers are contacted by the financial institution that they learn they may have been a victim of identity theft, giving them the opportunity to remedy the effects of identity theft sooner rather than later. In addition, most innocent victims have been and continue to be extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is a target or potential target of a phishing attack. Also, agreement from the operators to take down websites quickly when there is clear violation of trademarks or indications of fraud is only a partial solution. Financial institutions still need the WHOIS information to address the other forms of abuse noted above.

About BITS

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS' member companies provide fuel for America's economic engine, accounting directly for $50.5 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Within BITS there are two working groups that have an interest in the WHOIS data—the information security experts who are involved in the BITS Security and Risk Assessment Working Group and the fraud reduction experts who are involved in the BITS Fraud Reduction Steering Committee (FRSC). The mission of the SRA is to strengthen the security and resiliency of financial services by a) sharing and developing best practices to secure infrastructures, products and services; b) maintaining continued public and private sector confidence; and c) providing industry input to government agencies and regulators on policies and regulations. The mission of the FRSC is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

Efforts to Strengthen Cyber Security, Reduce Fraud and Mitigate Identity Theft

The financial services industry has been aggressive in its efforts to strengthen cyber security, reduce fraud, and mitigate identity theft. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud

and identity theft. As just one example of these efforts, the Identity Theft Assistance Center (ITAC), which BITS and the Financial Services Roundtable established in 2004, announced in March that it had helped over 5,000 individuals to restore their financial identity. These services are provided free to consumers by ITAC members.

We have included a detailed summary of BITS' efforts to address information security, fraud reduction and critical infrastructure protection in the appendix.

While we understand that the public comment period officially closed on February 8, 2006, we are hoping that ICANN will consider this input from information security and fraud risk experts of the largest financial services companies who are the "front lines" of the identity theft and Internet fraud battlefield. If you have any further questions or comments on this matter, please do not hesitate to contact me or John Carlson at john@fsround.org or 202-289-2442.

Sincerely,

Catherine A. Allen
CEO, BITS

Appendix: Protecting the Critical Infrastructure: BITS' Accomplishments in 2005

BITS
FINANCIAL SERVICES
ROUNDTABLE

APPENDIX: PROTECTING THE CRITICAL INFRASTRUCTURE: BITS' ACCOMPLISHMENTS IN 2005

PUBLICATIONS OF BEST PRACTICES AND GUIDELINES

Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy

- The BITS study on "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy" outlines inefficiencies resulting from regulatory overlap within:
  - The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA);
  - The Gramm-Leach-Bliley Act of 1999 (GLBA);
  - The Sarbanes-Oxley Act of 2002 (SOX); and
  - The proposed U.S. Inter-agency Operational Risk Supervisory Guidance on Operational Risk Advanced Measurement Approaches (AMA) for Regulatory Capital (applying the International Convergence of Capital Measurement and Capital Standards: A Revised Framework, also referred to as Basel II), July 2003.
  - The study includes specific recommendations for implementation by member institutions to increase efficiencies, and further provides recommendations for regulators to work with the financial services industry to reduce unnecessary burdens and eliminate inconsistent requirements. The study was made available in hard copy and jointly distributed by BITS and the Roundtable to key regulators as well as member institutions in a public launch event held October 11.

BITS Consumer Confidence Toolkit and Voluntary Guidelines

- BITS has developed a *Consumer Confidence Toolkit: Data Security and Financial Services.* This Consumer Confidence Toolkit is publicly available and provides information to support consumer confidence in the safety, soundness and security of financial services. Special attention is placed on online financial services transacted through the Internet. Data in support of the safety of online financial transactions are provided. Information about the proactive leadership of the financial services industry is included, as well as a description of the current environment and recommendations for government agencies and leadership. Tips for consumers to help protect their financial security, including in the online environment, are also provided. In addition, BITS has developed Voluntary

Guidelines as recommendations to member institutions for managing information security and consumer confidence issues.

Protecting the Elderly and Vulnerable

- BITS released a new tool in October 2005 to help reduce fraud. The publication, "BITS Fraud Protection Guide: Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation," describes the growth of this fraud, highlights ways to detect and prevent it, and urges financial institutions to work proactively to reduce it. "This new BITS publication serves to protect some of our nation's most vulnerable populations and reinforces our member institutions' 24/7 commitment to safe and secure financial transactions," said BITS CEO Catherine A. Allen. In the coming months, BITS will release a toolkit for educating financial center and loss management personnel on ways to identify and prevent this type of financial crime. The Financial Services Industry Toolkit provides information to support the implementation or improvement of a financial institution internal prevention program for education and awareness to protect the elderly and vulnerable from financial fraud.

E-Scams

- BITS formed a subcommittee under the auspices of the Internet Fraud Working Group to address the various scams operating throughout the Internet today. The BITS e-Scams Subcommittee was comprised of e-commerce specialists from more than 30 financial institutions. The e-Scams Subcommittee's goal was to provide information and best practices to BITS members and the financial services community in order to protect customers and enhance confidence in the Internet as a medium for online financial services. The result is a Members Only document that: defines the current landscape; assesses the impact of e-scams on financial institutions; reviews current industry technology solutions; provides an overview of an e-scam program with an emphasis on e-scam investigations; discusses outsourcing e-scams management; and outlines internal and external education and awareness programs. A final document is due for release in December 2005.

Back-Up Power Issues

- The *BITS Guide to Business-Critical Enterprise Power* (the *Guide*) is in draft. It provides financial institutions with industry business practices for understanding, evaluating and managing risks if the availability of the electrical system is disrupted. Further, it outlines ways financial institutions can enhance reliability and ensure uninterrupted back-up power, referred to as "enterprise power." The *Guide* is written for interested parties—from CEOs to business managers, risk managers to business continuity professionals, procurement experts to facilities managers—as they analyze risks, conduct due diligence for enterprise power and integrate evolving regulatory and building code requirements into business continuity plans. The final Guide will be available early in 2006. The full draft, completed in 2005, is being used and vetted currently.

BITS Critical Success Factors for Security Awareness & Training Programs

- Under the auspices of the BITS Security and Risk Assessment Program, BITS developed a description of critical factors for establishing and maintaining a comprehensive security awareness and training program for financial institution personnel. Developing a comprehensive security awareness and training program is a regulatory requirement and an effective risk management practice.

BITS Key Considerations for Global Background Screening Practices.

- BITS released the *BITS Key Considerations for Global Background Screening Practices* on June 29, 2005. This document is an outstanding tool for financial institutions and other critical infrastructure companies seeking to mitigate risks related to global outsourcing. The paper is divided into three sections:
  - Overview of the financial industry's legal and regulatory requirements;
  - Strategies for evaluating the risks and mitigating controls for outsourced environments and activities; and
  - Information to validate identity and background, listed by country.
- Each section outlines financial institutions' top considerations for global employee screening policies, programs and requirements. The paper is available on the BITS website at www.bitsinfo.org on the publications page.

Key Contractual Considerations for Developing an Exit Strategy

- Published in May, 2005, the *BITS Key Contractual Considerations for Developing an Exit Strategy* provides detailed suggestions for contracts with third party service providers. For all critical infrastructure companies, developing an exit strategy at the onset of the relationship can help the organization effectively manage risk and ensure continuity of service.

Strategies for Mitigating Fraud Risks Associated with the Check Clearing for the 21st Century Act

- This paper provides informed analysis of the risks and benefits associated with implementation of the Check 21Act. Strategies for mitigating risks are included as well as a matrix that describes Check 21-related risks and mitigants from the standpoint of three major parties affected by the Act: the business customer that truncates checks before deposit, the bank of first deposit, and the paying bank.

Fraud Prevention Strategies for Consumer, Commercial and Mortgage Loan Departments

- Loan fraud is a fast-growing problem. This Members' Only guide helps financial institutions catch loan frauds as they happen and recover from related losses. Members interested in obtaining a copy may access it via the BITS site, www.bitsinfo.org, in the Members Only area.

BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings

- In January 2005 BITS published the *BITS Guide to Verification, Authentication and Financial Experience Information Technology for Online New Account Openings.* This Members' Only guide assists financial institutions in understanding technology to verify and authenticate online users and determine the level of risk users pose to the institution. This document was created to help financial institution fraud managers as they explore these technologies and identify those that may be appropriate for their needs. This paper focuses on technology solutions for:
  - Verification. These products screen data elements provided by a client to ensure the elements (Social Security numbers, addresses, etc.) are real.

- Authentication. Once the data elements are verified, authentication products ensure the credentials given belong to the person providing them.
- Financial experience information. Having verified the data elements and authenticated the customer, financial experience information determines the level of risk assumed by accepting the potential customer.

BITS Kalculator: Key Risk Management Tool for Information Security Operational Risks

- The *Kalculator* starts with a list of common information security threats and vulnerabilities and matches them with corresponding controls to mitigate those risks. Using the *Kalculator*, financial institutions score their information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. Companies can use the results to boost their ability to assess and mitigate risks. The *Kalculator* is unique in that it brings together information security risk categories from international security standards and emerging operational risk regulatory requirements into one tool that can be easily customized.

Developing a KRI Program: Guidance for the Operational Risk Manager

- The document, *Developing a KRI Program: Guidance for the Operational Risk Manager*, helps operational risk managers establish and maintain strong KRI programs in an environment of increased operational risk regulation.

Best Practices in Patch Management for the IT Practitioner

- *BITS Best Practices in Patch Management* provides critical recommendations for an enterprise approach to managing patches. Divided into 10 sections reflecting the components of effective patch management processes, the document provides considerations for defining roles, responsibilities and tools; developing and maintaining an inventory of IT infrastructure; developing a "standard build"; and verifying patch installation. While created for financial institutions, these recommendations may be applied to other industries.

BITS IT Service Providers Expectations Matrix

- The BITS *IT Service Provider Expectations Matrix* provides financial institutions, service providers, and audit and assessment organizations with comprehensive and consistent expectations to reduce risk. Presented in an Excel spreadsheet, it outlines financial institution expectations for the security of information and personnel, as well as policies and processes for ensuring physical security. The expectations address critical disaster recovery/business continuity issues necessary to ensure products and services are supported by and coordinated with service providers.

BITS Guide to Business-Critical Telecommunications Services

- On November 15 of 2004, BITS released the *BITS Guide to Business-Critical Telecommunications Services*, however it has received continued use and additional visibility in 2005, including as a helpful tool in the aftermath of Hurricanes Katrina, Rita and

Wilma. The *BITS Guide* highlights questions business continuity planners and other risk managers should ask themselves as well as an overview of key points to consider in risk assessment, due diligence, contracting, testing and monitoring processes of their telecommunications services.

COMMENT LETTERS

Comment Letter on FDIC Study, "Putting an End to Account-Highjacking Identity Theft"

- BITS, The Financial Services Roundtable and the Identity Theft Assistance Corporation jointly submitted a comment letter, raising concerns about the proposed approach to remedies for fraud-related security risks. The study did not adequately take into account the fact that financial institutions are applying a risk-based approach for evaluating the risks, deploying controls and offering convenient solutions to their customers and recommended solutions that are complex, unwieldy, and, in some instances, will not provide the intended remedy.

Comment Letter on Department of Homeland Security (DHS) Interim Rule on Procedures for Handling Critical Infrastructure Information

- BITS and The Financial Services Roundtable submitted a comment letter to DHS on a rule to establish "uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security." The letter outlines concerns about the scope and implementation of the procedures. It states that DHS must implement robust controls to adequately protect employees and customers of financial institutions.

TESTIMONY

Hearing on "Continuity of Operations in the Financial Services Sector Post a Major Event," to the House committee on Government Reform Subcommittee on Government Management, Finance, and Accountability

- On September 26, BITS CEO Catherine A. Allen testified at a field hearing in New York City on the current status of financial market preparedness for wide-scale disasters and disruptions. The hearing was held by the House Committee on Government Reform Subcommittee on Government Management, Finance, and Accountability. Cathy's testimony focused on actions the financial services sector has taken in response to the 9/11 terrorist event and natural disasters such as Hurricanes Katrina and Rita. She praised the financial services' sectors preparedness and responsiveness and offered recommendations for additional steps that need to be taken by the Federal government and all critical infrastructure sectors. Cathy made specific recommendations for maintaining diverse and resilient communications channels, investing in the power grid, recognizing the dependence of all critical infrastructures on software operating systems and the Internet, and improving coordination among all critical infrastructures and with federal, state, and local government when events occur. She emphasized the importance of addressing the interdependence of all critical infrastructure sectors. Those of greatest concern to the financial services sector are interdependencies with telecommunications, energy and transportation sectors. For access to Cathy's full testimony, go to http://www.bitsinfo.org/p_public_testimony.html.

"The Department of Homeland Security Cybersecurity Enhancement Act of 2005" to House Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity

- Catherine A. Allen, BITS CEO, testified in April, 2005 on the importance of elevating the position of Cybersecurity Director at the Department of Homeland Security to an Assistant Secretary level. Her testimony included a description of the current cybersecurity landscape, and what BITS and the industry are doing to address threats. The testimony also included the BITS recommendations to the government to strengthen cybersecurity, referred to in detail and presented as the acronym PREPARE©.

SUMMITS, FORUMS AND CONFERENCES

Critical Infrastructure Protection

- BITS CEO Catherine A. Allen participated as one of four panelists at an event convened by George Mason University's Critical Infrastructure Protection Program at the National Press Club on November 29, 2005. Award-winning journalist Frank Sesno moderated the panel, "After the Storms, Repairing the Damage." James Lee Witt, former FEMA Director, keynoted the event. Other panelists were Dennis Barbour, Mayor of Carolina Beach, NC and J. Michael Hickey, Verizon. Catherine drew on lessons learned by the financial services sector, and stressed the continuing need to address issues of interoperability, interdependence with other sectors, implementation of lessons learned, and consumer confidence.
- BITS Senior Director John Carlson participated in the Vanderbilt University-hosted US Japan Critical Infrastructure Protection Forum on November 29 and 30, 2005 in Washington, DC. John spoke about BITS' efforts in cross-sector coordination among critical infrastructure sectors and cybersecurity and participated in a panel discussion on business continuity planning and response from a multi-day regional power outage scenario. The forum fostered dialogue between US and Japanese industries on how best to protect infrastructures that support those nation's economies. Speakers included senior US and Japanese government and private-sector officials and experts in financial services, information technology, power, telecommunications and transportation. For more information, contact John Carlson, john@fsround.org.
- John Carlson represented BITS at three meetings on July 11, August 12 and September 30, 2005 with senior Department of Homeland Security officials and over a dozen associations representing the business, IT and telecommunications industries. The purpose of the meetings was for the Department of Homeland Security to get input and recommendations from association leaders who are active in cyber security issues and to discuss how best to assess cyber security risks, improve the public/private partnership, expand information sharing, and develop public and private incentives to encourage government and the private sector to enhance cyber security.
- On June 17, 2005 Dartmouth's Institute for Information Infrastructure Protection (I3P) hosted a forum on "Financial Services Challenges in the Cyber World" at New York University in New York City. BITS participated in a panel discussion along with representatives from BITS member companies and key federal government agencies. Approximately 25 government and academic leaders involved in research on cyber security and critical infrastructure issues participated in the meeting.

- BITS held conference calls with senior business continuity planning and fraud reduction officials of member companies to discuss the impact of Hurricane Katrina on members and the financial services sector overall as well as relief efforts. BITS disseminated daily updates to members beginning on September 1, serving as a repository and conduit for timely information. BITS worked closely with the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and disseminated key information to our members from regulatory agencies, Treasury and the Department of Homeland Security. Topics included assessment of impacts from the storm, efforts to deliver adequate cash supplies, FEMA's distribution of debit cards to victims of Katrina, talking points for consumer assistance, guidance from regulatory agencies, and important contacts for additional support. BITS also helped develop a press release that was issued by the FSSCC and outlined the sector's efforts to respond to the crisis. This information-sharing and coordinating role continued through Hurricanes Rita and Wilma on an as-needed basis. BITS also worked with the FSSCC to develop a memo on lessons learned from the Hurricanes that was send to Treasury and the FBIIC.

A Strategic Look at Authentication

- On March 8, 2005, BITS hosted a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum focused on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

BITS Regulatory Forum

- The BITS Regulatory Forum was held on April 26, 2005 and established a dialogue among regulators and financial services firms on the impact of regulatory requirements and supervisory processes. Many of those requirements relate to critical infrastructure protection and security issues. Participants reviewed steps to be taken by all parties to increase efficiency in the regulatory and supervisory process. Senior level regulators and BITS members took part in this session, the first step in an iterative, cross-sector process. The Forum was the first public release of the study, developed on BITS' behalf by KPMG, "Reconciliation of Regulatory Overlap for the Management and Supervision of Operational Risk in US Financial Institutions: Improving Compliance Efficiencies by Minimizing Redundancy"

BITS/American Banker Financial Services Outsourcing Conference

- The Fourth Annual BITS/American Banker Outsourcing Conference, presented with The Santa Fe Group in 2005, was held on November 7 - 8 at the Renaissance in Washington D.C. This year's agenda followed four key themes:
  - Governance: Best practices of financial institutions and service providers.
  - Compliance: Strategies for negotiating the current landscape and requirements for privacy and security.
  - Risk Management: Strategies, controls and processes to coordinate risk management across the enterprise.
  - Change: Practical guidance for managing today's dynamic relationships.

POLICY DEVELOPMENT

NOTE: BITS serves as a source of fact-based information in the development of policy positions. Following are recent examples, resulting either in a formal position from both BITS and The Financial Services Roundtable, or indirectly, through participation in national-level councils, working groups and task forces. Other examples of BITS' role in policy development are listed above in the categories of Comment Letters and Testimony.

- Joint BITS and Financial Services Roundtable Policy on Authentication Mandates
- Joint BITS and Financial Services Roundtable Policy on Spyware
- Joint BITS and Financial Services Roundtable Policy on Software Security
- Joint BITS and Financial Services Roundtable Policy on Internet Fraud and Phishing
- Support for President's National Infrastructure Advisory Council (NIAC)
- Participation in National Security Telecommunications Advisory Council (NSTAC) Financial Services Task Report
- Participation in Network Reliability and Interoperability Council (NRIC) VII
- Participation in Congressman Adam Putnam's Corporate Information Security Working Group (CISWG)
- Participation in the National Cyber Security Partnership

PILOTS AND PROJECTS

Financial Institutions Shared Assessments Project (FISAP)

- BITS has recently launched a new project aimed at improving efficiencies and achieving cost savings related to assessments of shared third party services providers. This Financial Institutions Shared Assessment Project (FISAP) is in pilot stage.
- Six institutions formed FISAP to leverage the *BITS Framework* and *BITS Expectations Matrix* and develop an industry solution for service provider assessments. Big Four firms are acting as Technical Advisors to the project. Critical success factors are to:
  - Develop reports that are comprehensive and suitable for multiple financial institutions;
  - Reduce the time and resources financial institutions and service providers spend responding to and executing one-off assessments to verify controls and security;
  - Create a process that is repeatable and consistent; and
  - Encourage support of regulators.
- The project is intended to result in significant cost savings and efficiency gains. These "shared assessments" are being developed to improve assessments based on consistent and objective information that is provided through a regularly-updated, standardized questionnaire as well as third-party testing and objective reporting on controls. It should be noted that FISAP is not a "100%" solution. The savings and efficiencies will fluctuate by risk, service and amount of dedicated vs. shared services. BITS expects to expand this project to additional participants in early 2006.

Anti-Phishing Efforts

- BITS is responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams,

BITS created a Phishing Prevention and Investigation Network. The BITS Phishing Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The BITS Phishing Network includes a searchable database of information from other financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Network also provides data on trends to help law enforcement build cases and shut down identity theft operations. The BITS Phishing Prevention and Investigation Network:

- Helps member institutions monitor and shut down e-scams faster and more effectively.
- Reduces financial institution manpower costs and losses.
- Increases phishing investigations and arrests of perpetrators.
- Facilitates communication among fraud specialists at financial institutions, service providers and law enforcement agencies.

ChicagoFIRST

- With the encouragement of the US Treasury and support from BITS, Chicago's premier financial services institutions formed ChicagoFIRST in July 2003 as an industry coalition that addresses homeland security issues requiring a common response by Chicago's financial services sector. In 2005, ChicagoFIRST became a model for a similar regional coalition in Florida. These initiatives are prompted by a consensus that existing activities at the regional level do not adequately address the critical infrastructure protection concerns of Chicago's financial institutions. The mission of ChicagoFIRST is:
  - To increase the resilience of the Chicago financial services industry in the event of a regional disaster in collaboration with the city, state and federal agencies, including to:
    - protect the lives of the thousands of people that work in the industry;
    - protect the financial assets that have been entrusted for safe keeping and investment;
    - work directly with city and state authorities on emergency coordination and evacuation; and
    - implement the primary objectives in a rapid manner.

  The "lessons learned" from ChicagoFIRST, as reported above and funded by the US Treasury, were published in December 2004, with the hope that additional coalitions will successfully establish similar organizations to strengthen critical infrastructures at a regional level. The Treasury supports the concept of regional coalitions of financial services firms and will work with interested parties to facilitate their formation. For more information, please contact the Office of Critical Infrastructure Protection and Compliance Policy at (202) 622-2602.

Identity Theft Assistance Center (ITAC)

- The Identity Theft Assistance Center (ITAC) was initiated as a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and by enabling law enforcement to identify and prosecute perpetrators of this crime. The ITAC is now officially up and running as the pilot was a success. As of August 2005, more than 2500 victims of identity theft had received assistance from the ITAC. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. The ITAC's services are free-of-

charge to customers and made available based on referrals to the ITAC by one of the ITAC's Members. For additional information, go to www.identitytheftassistance.org.

BITS Product Certification Program (BPCP)

- The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency and National Institutes of Technology and Standards.

Joint Work Plans with Major Software Providers

- BITS' efforts to improve the quality of software security have three overarching objectives. BITS wants vendors to provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; ensure products comply with security guidelines before releasing products; and make the patch-management process more secure and efficient and less costly for organizations. To meet these objectives, BITS is urging vendors to comply with business requirements. Under the requirements, software vendors would use security criteria, like the BITS software security criteria and the Common Criteria, in developing software products to ensure products meet minimum security standards. Companies would then test the products for security and conduct thorough code reviews prior to releasing them. To facilitate achievement of these objectives, BITS has implemented a joint work plan with one major software provider and is developing joint work plans with others.

SURVEYS AND RESEARCH

Cybersecurity R&D Priorities.

- The results of a 2005 BITS survey on cybersecurity research and development are being used to advise the federal government (Congress, Treasury, the Department of Homeland Security) on its R&D priorities. The BITS survey coincides with the publication of a Cyber Security Industry Alliance (CSIA) paper urging the federal government to play a larger role in coordinating cybersecurity R&D funding. The CSIA paper notes that while the private sector contributes the majority of funds for R&D on cybersecurity, most of this money is for short-term solutions to existing problems. The CSIA and BITS are recommending the federal government organize long-term cybersecurity research to address problems before they emerge.

FOR ADDITIONAL INFORMATION, CONTACT:

Catherine A. Allen, CEO
John Carlson, Senior Director
BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington DC 20004

(202) 289-4322
cathy@fsround.org
www.bitsinfo.org

ABOUT BITS

BITS was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. For more information, go to www.bitsinfo.org.

June 22, 2006

To: Internet Corporation for Assigned Names and Numbers
U.S. Government Agencies involved in an ICANN Working Group (Commerce Department, Federal Bureau of Investigations, Federal Trade Commission, Homeland Security Department, and State Department)

Re: WHOIS Data Base

Dear Sirs and Madams:

The purpose of this letter is to express the concern of members of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) on the proposal before the Internet Corporation for Assigned Names and Numbers (ICANN) to limit the type of information collected and maintained in the WHOIS data base. Based on a review of the information provided in the January 18, 2006 task force report containing two opposing formulations of the "purpose of WHOIS," and discussions among information security and fraud risk managers, we urge ICANN to adopt Formulation 2.[1] Formulation 2 will provide financial institutions with the information they need to respond to identity theft and account fraud.

Under formulation 1, the only purpose of WHOIS is to "resolve issues related to the configuration of the records associated with the domain name within a DNS nameserver" (i.e., narrow technical issues). Under formulation 2, the purpose of WHOIS is to help resolve a broader range of "technical, legal or other issues regarding registration or use of a domain name." We believe the adoption of formulation 1 would make it more difficult and time-consuming for financial institutions to identify and stop domain-based scams and the identity theft and account fraud that result.

Financial institutions have always been a favorite target for perpetrators of fraud. Institutions have long answered this challenge with reliable business controls, advanced technology, information sharing, and cooperative efforts with government and law enforcement agencies. Further, financial institutions must also deal with other domain-based issues including, but certainly not limited to, trademark infringement, unauthorized and sometimes unlawful disclosure of confidential, proprietary or customer information, spam attacks, inappropriate content sent or received via email, and violation of intellectual property rights by web site operators. While our members' foremost concern is to protect their customers and maintain their trust, they must also be mindful of the need to comply with the requirements set forth by numerous laws, regulations and supervisory guidance.

We believe that formulation 1 (or other efforts to limit or narrow the information) in WHOIS could adversely affect the financial services industry's efforts to respond to identity theft and phishing attempts. Timely response to phishing attacks and identity theft is critical to protect customers, financial institutions, and innocent consumers who may not be aware of their victimization. In many cases, the only tool financial institutions have for identifying registrants or purported registrants of domain names in a timely manner is via the WHOIS contact information. Often times, the fraudsters will register a domain name in the name of innocent consumers without the knowledge of the consumer. In most instances, it is not until

[1] http://www.icann.org/announcements/announcement-18jan06.htm)

these unsuspecting consumers are contacted by the financial institution that they learn they may have been a victim of identity theft, giving them the opportunity to remedy the effects of identity theft sooner rather than later. In addition, most innocent victims have been and continue to be extremely helpful to financial institutions in taking down or transferring these domain names to the financial institution that is a target or potential target of a phishing attack. Also, agreement from the operators to take down websites quickly when there is clear violation of trademarks or indications of fraud is only a partial solution. Financial institutions still need the WHOIS information to address the other forms of abuse noted above.

About FSSCC

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (www.fsscc.org) is a group of private-sector firms and financial trade associations that works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. In this capacity, FSSCC works with the Department of Treasury, which has direct responsibility for infrastructure protection and homeland security efforts for the financial services sector. It serves under the overall guidance of the Department for Homeland Security, under Homeland Security Presidential Directive 7. Since most of the sector is privately owned, the Treasury Department appoints a private-sector coordinator with whom to work on these issues. The current FSSCC Chairman is George Hender, Management Vice Chairman of The Options Clearing Corporation, who was appointed to this role on June 6, 2006 by U.S. Treasury Secretary John Snow. The following associations and organizations are FSSCC members:

American Bankers Association
America's Community Bankers
American Council of Life Insurers
American Insurance Association
American Society for Industrial Security International
BAI
BITS/The Financial Services Roundtable
The Bond Market Association
ChicagoFIRST, LLC
Chicago Mercantile Exchange
The Clearing House
CLS Services
Consumers Bankers Association
Credit Union National Association
The Depository Trust & Clearing Corporation
Fannie Mae
Financial Information Forum
Financial Services Information Sharing and Analysis Center, LLC
Financial Services Technology Consortium
Futures Industry Association
Independent Community Bankers of America
Investment Company Institute
Managed Funds Association
NACHA – The Electronic Payments Association
The NASDAQ Stock Market, Inc.
National Association of Federal Credit Unions
National Association of Securities Dealers
New York Board of Trade

The Options Clearing Corporation
Securities Industry Association

We appreciate your attention to this matter. If you have any further questions or comments on this matter, please do not hesitate to contact me at 312-322-4513 or ghender@theocc.com, or Dave Engaldo at 312-322-2002 or dengaldo@theocc.com.

Sincerely,

George Hender

George Hender
Chairman, FSSCC

InterContinental Hotels Group
Three Ravinia Drive
Suite 100
Atlanta, GA 30346-2149
www.ichhotelsgroup.com

Eric Pearson
Senior Vice President
Global Distribution Marketing

June 22, 2006

Via FedEx
Mr. Vinton G. Cerf
Chairman of the Board
ICANN
c/o Google
13800 Coppermine Road
Suite 384
Herndon, Virginia 20171
(Also via e-mail: vint@google.com)

Via FedEx
Dr. Paul Twomey
President and CEO
ICANN
4676 Admiralty Way
Suite 330
Marina del Rey, California 90292-6601
(Also via e-mail: twomey@icann.org)

Re: The purpose of Whois and of the Whois contacts

Dear Mr. Cerf and Dr. Twomey:

I am writing to you on behalf, and in my capacity as chair, of the Hotel Consumer Protection Coalition ("HCPC"), an organization described in more detail below whose current members are Global Hyatt Corporation; InterContinental Hotels Group; Marriott International, Inc.; and Starwood Hotels & Resorts Worldwide, Inc. Collectively, our companies include more than 6,600 hotels in more than 100 countries.

I am writing with regard to the ongoing debate about the "purpose of Whois and of the Whois contacts" and, in particular, the two formulations that have been offered by the ICANN GNSO's preliminary task force (http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-18jan06.htm).

The HCPC addresses industry-wide problems arising from e-commerce practices that harm or mislead consumers, and in turn damage the reputation of coalition member companies, their brands and the hospitality industry as a whole. Coalition activities focus on the research and resolution of unfair, false, misleading or deceptive online practices and marketing-related activities. The coalition also intends to educate consumers on such practices and how to protect themselves and to work with government authorities and other appropriate entities to reduce harmful e-commerce-related activities.

InterContinental Hotels Group
Three Ravinia Drive
Suite 100
Atlanta, GA 30346-2149
www.ichhotelsgroup.com

Eric Pearson
Senior Vice President
Global Distribution Marketing

The HCPC strongly supports "Formulation 2" for the purpose of Whois and of the Whois contacts, which states:

> The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party or parties for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, technical, legal or other issues related to the registration or use of a domain name.

The addition of the word "legal" to Formulation 2, which is missing from Formulation 1, is a key difference that is of vital importance to our hotel consumers, the general public and the companies we represent.

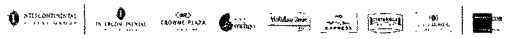
To protect our hotel consumers, members of the HCPC use Whois repeatedly on a daily basis to identify domain name registrants and website operators that are creating websites using our trademarks to mislead consumers. Given the large number of hotel consumers we serve and the well-known brands represented by members of the HCPC – including, among others, Holiday Inn, InterContinental, Crowne Plaza, Marriott, Ritz-Carlton, Sheraton, Westin, W Hotels, Hyatt and AmeriSuites – our hotel consumers and our companies are prime targets for cybersquatters, phishers, spammers and other bad actors on the Internet.

To help shield our hotel consumers from such illegal activities on the Internet, all members of the HCPC have filed complaints under ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP") to obtain the transfer of domain names that were being used by others in bad faith. For example:

- To protect hotel consumers from viewing a pornographic website using its famous Holiday Inn trademark in a domain name, Six Continents Hotels, Inc. ("SCH") (an InterContinental Hotels Group company), recently obtained the transfer of the domain name <holidayinnmanassas.com>. *Six Continents Hotels, Inc. v. CredoNIC.com / Domain For Sale*, WIPO Case No. D2005-0755. SCH has also obtained the transfer of numerous other domain names through the UDRP process and in other ccTLDs.

- To protect hotel consumers who use its popular frequent traveler program known as Marriott Rewards, Marriott International, Inc., obtained the transfer of the domain name <marriottreward.com>. *Marriott International, Inc. v. Thomas, Burstein and Miller*, WIPO Case No. D2000-0610.

- To protect hotel consumers from being misled by a website that used its well-known Hyatt Regency trademark in the domain name and redirected visitors to hotel and travel services in competition with its hotel and travel services, Hyatt Corporation obtained the transfer of the domain name <hyattregency.com>. *Hyatt Corporation v. NA*, WIPO Case No. D2005-0419.



INTERCONTINENTAL HOTELS GROUP

InterContinental Hotels Group
Three Ravinia Drive
Suite 100
Atlanta, GA 30346-2149
www.ichhotelsgroup.com

Eric Pearson
Senior Vice President
Global Distribution Marketing

- To protect hotel consumers from a single registrant who used multiple domain names that all contained the names of its hotel brands, Starwood Hotels & Resorts Worldwide, Inc., obtained the transfer of 28 domain names that were used in connection with competing services. *Starwood Hotels & Resorts Worldwide, Inc. v. Domaincar*, WIPO Case No. D2006-0136.

In addition to using Whois to identify the domain name registrants in the UDRP cases listed above, members of the HCPC also regularly use Whois to contact domain name registrants and successfully negotiate the voluntary transfer of problematic domain names without incurring the time and expense of the UDRP process. Furthermore, members of the HCPC also regularly use Whois for other legal purposes, such as to identify copyright infringers and others who are violating our companies' legal rights.

Without the benefit of unrestricted access to a database of information about, and contact information for, domain name registrants, we would find it difficult, if not impossible, to protect the public and enforce our rights on the Internet as we currently do. Any effort to reduce the amount of information in the Whois database or to limit our access to it would undermine our ability to assert our legal rights; consequently, our consumers would be harmed by, for example, being led to pornographic and inappropriate websites. Furthermore, our consumers might be forced to bear the burden of the increased financial expenses we would have to incur to identify website operators through court proceedings and private investigations if the Whois database were modified.

At the very least, we believe that accessibility to the existing types of information in the Whois database should remain as-is. We also have serious doubts about the existing accuracy and reliability of this database and its abuse by domain name registrants. For example, in one UDRP case filed (and won) by HCPC member InterContinental Hotels Group's Six Continents Hotels, Inc., the registrant was listed in Whois as, literally, "Sdf fdgg" – an obvious random typing of characters on a computer keyboard. (The domain name was being used in connection with a website that automatically redirected users to a site that contained pornographic images of partially clothed people urinating, and links to other pages, including those labeled "Rape Site" and "Incest & Mature Site.") *Six Continents Hotels, Inc. v. Sdf fdgg*, WIPO Case No. D2004-0384.

We have heard concerns that publicly available information in the Whois database should be limited to safeguard the privacy of domain name registrants. However, existing systems already exist for this purpose, through the so-called "domain proxy" or "domain privacy" services offered by many registrars that mask the true identify of their registrants. Therefore, no change to the Whois system is necessary to safeguard the privacy of domain name registrants, as such a system already exists.

In light of the above, for the protection of our consumers, the public and our companies – as well as for **the overall integrity of the Internet** – the Hotel Consumer Protection Coalition strongly encourages you to support Formulation 2 for the purpose of Whois and of the Whois contacts, to

INTERCONTINENTAL HOTELS GROUP

InterContinental Hotels Group
Three Ravinia Drive
Suite 100
Atlanta, GA 30346-2149
www.ichhotelsgroup.com

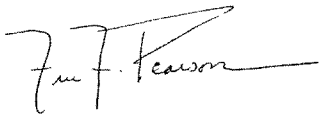
Eric Pearson
Senior Vice President
Global Distribution Marketing

ensure the continued unrestricted access to the Whois database and to take all steps practical to improve the accuracy and reliability of Whois data.

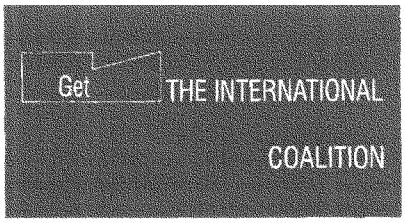
We greatly appreciate your consideration of our views, and we would welcome the opportunity to discuss this issue further with you in any appropriate forum.

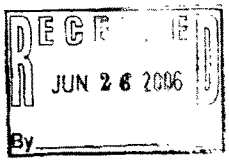
Sincerely,

FOR THE HOTEL CONSUMER PROTECTION COALITION



Eric Pearson
Senior Vice President, Global Distribution Marketing, InterContinental Hotels Group
Chair, Hotel Consumer Protection Coalition





Mr. Vinton G. Cerf
Chairman of the Board
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way
Suite 330
Marina del Rey, CA 90292-6601

E-mail: vint@google.com

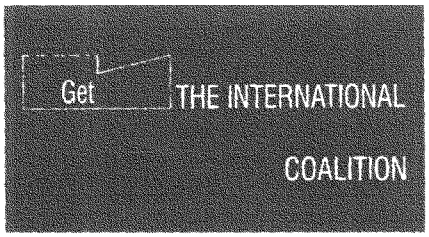
Dear Mr. Cerf:

On behalf of the International AntiCounterfeiting Coalition (IACC), I write to express my strong concerns about the proposal to re-define the purpose of the Whois service as limited to the resolution of technical issues. I believe this step would have a detrimental impact on accountability and transparency on the Internet, and as such would definitely be the wrong step for ICANN to take on this important matter.

The IACC is the largest multinational organization representing exclusively the interests of companies concerned with product counterfeiting and copyright piracy. Our members consist of approximately 150 corporations, trade associations, and professional firms and represent total revenues of over $650 billion. The IP owners among our membership represent a broad cross-section of industries, and include many of the world's best known companies in the apparel, automotive, consumer goods, entertainment, pharmaceutical, personal care and other product sectors.

The IACC is committed to working with partners from government, industry, and non-governmental organizations around the world to strengthen IP protection by encouraging improvements in the law, allocation of greater political priority and resources, and raising awareness regarding the enormous—and growing—harm caused by IP violations. Current estimates place the global trade in counterfeits in excess of $400 Billion; online counterfeiting sales are believed to account for approximately 10% of that total.

In response to the rising use of the Internet to facilitate such illegal activity, IACC members are accelerating their efforts to combat the advertising and sale of counterfeit goods online. In so doing, they rely heavily upon ready access to Whois – the database



of contact information on domain name registrants. Consulting Whois is a step taken in virtually every investigation of online counterfeiting. In some cases it is a critical step that leads rapidly to a resolution of the problem. Even where it does not, it can provide valuable information for identifying counterfeiters and conducting investigations that are ultimately turned over to law enforcement authorities.

Without unimpeded access by brand owners to Whois data, the investigation and resolution of these cases, with or without criminal prosecution, would certainly be slower, more costly and less effective than it is today.

Counterfeiting and piracy online are not "technical issues." They are violations of private rights and of public laws that have the purpose of protecting consumers against fraud, misrepresentation and abuse. In many cases, counterfeiting threatens not only the integrity of the marketplace -- especially the online marketplace -- but also public health and safety. Restricting the data in publicly accessible Whois to the information needed to resolve technical problems would certainly set back the fight against counterfeiting and piracy that is being waged worldwide. If that were to occur, the general public would bear the brunt of the costs.

We understand that ICANN's consideration of this issue is ongoing and that no final decision has been made. We also recognize that the status quo could be improved in many respects --- notably, with regard to the accuracy and reliability of Whois data -- and welcome consideration of such improvements within ICANN. However, we believe the consequences of the adoption of the narrow formulation of the purpose of Whois would be so detrimental that we felt it necessary to bring them to the attention of the members of the ICANN's Board as promptly as possible. We respectfully urge you and your colleagues to keep these considerations in mind as this discussion continues.

Respectfully submitted,

Nils Victor Montan
President

IFA
INTERNATIONAL FRANCHISE ASSOCIATION

EXECUTIVE COMMITTEE
Lawrence "Doc" Cohen, CFE
Doc & Associates
Chairman
Michael Seiferth, CFE
ServiceMaster Clean and
Furniture Medic
1st Vice Chairman
Steven J. Brooksbank, CFE
PostNet International Franchise
Corp.
2nd Vice Chairman
Dina Dwyer-Owens, CFE
The Dwyer Group
Secretary
Russell J. Frith, CFE
Liberty Digital
Treasurer
Richard Arnold, CFE
Ameritrax Loss Prevention
Immediate Past Chair
Sidney Feltenstein
Right Choice Brands
Past Chair
Jack Faris
Faris Enterprises
Chairman, Franchisee Forum
Stephen Joyce
Mail-Well International
Chairman, Franchisor Forum
Brad Haiman
Hollman Public Relations
Chairman, Supplier Forum

BOARD OF DIRECTORS
Jeff Anderson
The UPS Franchise Advisory
Council
Ron Berger
Pilgrim's Pantry Pizza, Inc.
Jerry Crandall, CFE
Jani-King International, Inc.
Richard Emerson
McDonald's Corp.
William B. Hall, CPA
William B. Hall & Co.
David Jordan
Pizza Fusion Franchise
Adam Khan
Falcon Holdings, LLC
Kirk Kinsell, CPA
InterContinental Hotels Group
William Koppel
Dunkin' Brands, Inc.
Dan Morton
UPS International, Inc.
1st Vice Chair, Supplier Forum
Eric McCarthy
The Coca-Cola Co.
David Middlebrooks
Lowe Doctor of Bloomquist Sharp
1st Vice Chair, Franchisee Forum
Barbara Moran
Moran Industries, Inc.
Geoffrey Oldaker, CFE
Mosaic Matter, LLC
Charles Rowley III
Yum! Brands Inc.
Rick Robinson
Jani-King Southwest
Steve Rogers
The Franchise Company, Inc.
Michael Renton, CFE
ExxonMobil Fuels Marketing
Steve Romanello, CFE
FOCUS Brands, Inc.
Heather Rowe
Sonic Realties
Ann Rosenberg, CPE
Rosenthal Winery LLC
Michael Seid, CPE
Michael H. Seid & Associates
Nikki Seitz, CPE
Express Personnel Services, Inc.
Larry Tay
Golden Corral Buffet & Grill
Kenneth Walker
Meineke Car Care Centers
Samuel Wright
Caldwell Corp.
George Zoggomo
7 Dimes Co.

Matthew H. Shay
President

June 19, 2006

Vinton G. Cerf
Chairman
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601

Dear Mr. Chairman,

On April 12th, 2006, the Generic Names Supporting Organization (GNSO) passed a resolution redefining the usage and purpose of the "Whois" database. By limiting the "purpose of Whois" to simply "resolve issues related to the configuration of records associated with the domain name within a DNS nameserver," the council has weakened the franchise community's tool to discover those who would use a domain name in a fraudulent and unethical manner. Changing the purpose of the Whois database eliminates the consumer's ability to investigate whether he/she is being misled or deceived.

The members of the franchise community regularly rely on the Whois database to:

- Identify parties responsible for the coordination of piracy or product counterfeiting via the World Wide Web
- Participate in e-commerce by learning the identities of suppliers and buyers
- Assist law enforcement, as well as consumer protection agencies, with the protection of consumers in cases of fraudulent websites

It is imperative that your council understand the absolute ramifications of this resolution. By closing the door on the public consumer and business community, you remove fundamental information that is used for the protection of commerce. This resolution will give anonymity to those that would use it to harm and defraud.

Franchised businesses' access to the Whois database ensures that the identities of customers are protected and the reduction of online fraud continues. If a consumer, or business, is defrauded online it hurts the party that created the counterfeit business as well as the entire business community. The prevention of fraudulent behavior enhances the integrity of the online business community. The current long-standing rules on access to Whois are the best way to fulfill this important consumer protection need and they should be maintained.

The International Franchise Association, therefore, strongly urges ICANN to reconsider the GNSO's resolution to redefine the purpose and use of the Whois database. We believe the preservation of current rules and access is in the best interest of every stakeholder. On behalf of the franchise community, we hope that ICANN will realize that recent actions will deeply and negatively effect the integrity of the business community and the public trust.

We thank you for this opportunity to express our concerns, and we are happy to assist you in every way possible to address these issues.

Regards,

David French
Vice President, Government Relations

World Headquarters: 1501 K Street N.W. Suite 350 Washington, DC 20005
Telephone: 202/628-8000 Fax: 202/628-0812 E-Mail: ifa@franchise.org Internet: www.franchise.org

WORLD FRANCHISE COUNCIL MEMBER

International Trademark Association
Representing the Trademark Community since 1878

Via Electronic Mail
vint@google.com

June 12, 2006

Vinton G. Cerf, Ph.D.
Chairman, Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6601

Dear Dr. Cerf:

The International Trademark Association (INTA) is extremely concerned about the April vote of the Generic Names Supporting Organization (GNSO) Council to recommend limiting the purpose of the Whois only to "resolve issues related to the configuration of records associated with the domain name within a DNS nameserver." INTA (http://www.inta.org) is a not-for-profit membership association of more than 4,900 trademark owners and professionals, from more than 180 countries, dedicated to the support and advancement of trademarks and related intellectual property as elements of fair and effective national and international commerce. As the ICANN Board monitors the ongoing policy development process regarding Whois, we respectfully request that it resolve to preserve access to registrant contact data in Whois and to improve the accuracy of that data so that violations of law and threats to the health and safety of the public may be addressed in an efficient manner.

Whois serves a vital role in remedying fraud on the Internet. Its uses include: law enforcement, consumer protection, and the protection of intellectual property rights. Trademark owners value Whois data in order to resolve domain name disputes (*e.g.*, cybersquatting) and learn the contact details for owners of websites offering dangerous counterfeit products. Only with access to accurate and up-to-date Whois data can the Internet be a safe environment that can be relied on with confidence.

Whois not only facilitates the investigation of legal violations on the Internet, but serves a basic function in making the rule of law apply to the Internet by providing information necessary to serve notice and institute legal action against violators. Similarly, the ICANN Uniform Dispute Resolution Policy, an anticybersquatting tool and one of ICANN's great successes, requires that complainants and dispute resolution providers serve notice of complaints upon domain name owners, using information found in the Whois database.

All these important uses would be impeded were the narrow formulation of the purpose of Whois to be implemented. Under that formulation, individuals and companies who have suffered legal injury from another's conduct on the Internet would be forced to commence court proceedings merely to find out the name of their alleged wrongdoer. This would result in unnecessary and expensive litigation and would not only impede a business whose trademark has been infringed or impermissibly incorporated into a domain name, but would also, for example, hamper a consumer fleeced by a faceless and unscrupulous merchant. The pace of Internet fraud and crime makes it crucial to obtain basic identifying information about the owner of a domain name. The GNSO Council's recommendation fails take into account the public interest in seeing online fraud, piracy, and crime investigated and remedied.

Investigation and remediation of domain name disputes would be facilitated not only by accessibility to Whois data, but by ensuring the accuracy of that data. We recognize and are grateful for ICANN's efforts in this area, including the Whois Data Reminder Policy, but note that our membership continues to advise us of blatantly false or missing Whois data that is not being corrected by registration authorities. Accordingly, as part of the overall consideration of Whois policy we ask that the Board implement additional tools to ensure Whois accuracy.

INTA is grateful for your attention to this crucial issue, and looks forward to assisting ICANN in the development of sound policy in this area. If you or another member of the ICANN Board has any questions concerning our position on Whois matters, please contact INTA External Relations Manager Michael Heltzer at mheltzer@inta.org.

Sincerely,

Paul W. Reidl
President

cc: Steve Metalitz, Esq., President, ICANN Intellectual Property Constituency
Lucy Nichols, Esq., ICANN Intellectual Property Constituency GNSO Council Representative
Ellen Shankman, Esq., Chair, INTA Internet Committee
Sarah Deutsch, Esq., Vice Chair, INTA Internet Committee

1201 New York Ave., NW
Washington, DC 20005
(202) 289-3120
(202) 289-3185 fax
www.ahla.com

June 22, 2006

Vinton G. Cerf
Chairman
Internet Corporation for Assigned Names and Numbers
4676 Admiralty Way
Suite 330
Marina del Rey, CA 90292-6601

Dear Mr. Chairman,

We are writing to express our serious concerns about a resolution adopted on April 12 by ICANN's Generic Names Supporting Organization (GNSO) to define the "purpose of Whois" as only to "resolve issues related to the configuration of records associated with the domain name within a DNS nameserver."

Those of us in the travel and hospitality industries depend on ready access to Whois data to enhance accountability and transparency online, and we believe such a policy change will have a seriously detrimental effect on our consumer protection efforts both in the U.S. and abroad.

Travel and hospitality companies use Whois in several ways: 1) to identify parties responsible for registration of misleading domain names, which are often the source of online frauds or phishing schemes; 2) to prevent or investigate misconduct facilitated by misleading registrations; 3) to cooperate with law enforcement to protect consumers in cases of fraudulent websites; and 4) to protect our legitimate intellectual property rights.

If the "purpose of Whois" is defined narrowly as proposed by GNSO, most of the data now in Whois would be cut off from public access - including data as fundamental as the name of the domain name registrant. If the change were to be implemented in new ICANN rules, most of the current public and business uses of Whois would become virtually impossible.

Consumer protection is the primary concern in Internet commerce. Our businesses need access to the Whois database to protect the privacy and security of our customers and to reduce the risk of online fraud, including identity theft. Internet users would lose significant privacy protections under the narrowly defined "purpose of Whois."

For example, cases of fraud or trademark infringement would not be considered "technical issues." Since time is of the essence in addressing these cases, we must be able to respond as quickly as possible. The current long-standing rules on access to Whois are the

best way to fulfill this important consumer protection need and they should be maintained.
We, therefore, strongly urge ICANN to reconsider the GNSO Council's April 12 resolution. We recommend that you preserve and enhance access to Whois data for purposes of protecting consumers and fighting fraud. We hope that ICANN will work to further enhance the accuracy of the Whois database. There is a tremendous public interest value in a rich Whois data set with information on registrants and administrative contacts.

We thank you for this opportunity to express our concerns, and we would be happy to assist you in every way possible to address these issues.

Sincerely,

Geoff Ballotti
President, North America Division
Starwood Hotels & Resorts Worldwide, Inc

Christopher L. Bennett
Executive Vice President and General Counsel Interstate Hotels & Resorts, Inc.

Lyle L. Boll
Sr. Vice President and General Counsel
Millennium Hotels and Resorts

Elisabeth Roth Escobar
Vice President & Senior Counsel, Intellectual Property Marriott International Inc.

Lynn Goodendorf
Vice President Information Privacy Protection InterContinental Hotels Group, Inc.

David Kong
President & CEO
Best Western International, Inc.

Joseph A. McInerney, CHA
President and CEO
American Hotel & Lodging Association

Scott McLester
Senior Vice President, Legal
Cendant Corporation, Inc.

Scott Normali
Senior Vice President
Distribution - Website Development & Marketing Hilton Hotels Corporation

Douglas Verner
Vice President, General Counsel & Secretary Guest Services, Inc.