AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ICANN INTERNET GOVERNANCE: IS IT WORKING?

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
AND
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 21, 2006

Serial No. 109-142

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

31-468PDF WASHINGTON : 2006

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

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

JAN SCHAKOWSKY, Illinois
Ranking Member
MIKE ROSS, Arkansas
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
BOBBY L. RUSH, Illinois
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan
(EX OFFICIO)

SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

FRED UPTON, Michigan, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
JOHN SULLIVAN, Oklahoma
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

EDWARD J. MARKEY, Massachusetts
Ranking Member
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
MIKE DOYLE, Pennsylvania
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

	Page
Testimony of:	
Kneuer, John M.R., Acting Assistant Secretary for Communications and Information, United States Department of Commerce	14
Twomey, Dr. Paul, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers	19
DelBianco, Steve, Vice President for Public Policy, Association for Competitive Technology, on behalf of NetChoice Coalition	25
Lenard, Thomas M., Senior Vice President for Research, The Progress & Freedom Foundation	37
Feld, Harold, Senior Vice President, Media Access Project	42
Bohannon, Mark, General Counsel and Senior Vice President, Public Policy, Software & Information Industry Association	61
Additional material submitted for the record:	
Kneuer, John M.R., Acting Assistant Secretary for Communications and Information, United States Department of Commerce, response for the record	93
Twomey, Dr. Paul, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers, response for the record	95
DelBianco, Steve, Vice President for Public Policy, Association for Competitive Technology, on behalf of NetChoice Coalition, response for the record	98
Lenard, Thomas M., Senior Vice President for Research, The Progress & Freedom Foundation, response for the record	101
Feld, Harold, Senior Vice President, Media Access Project, response for the record	102
Bohannon, Mark, General Counsel and Senior Vice President, Public Policy, Software & Information Industry Association, response for the record	103

ICANN INTERNET GOVERNANCE: IS IT WORKING?

THURSDAY, SEPTEMBER 21, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
AND
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET,
Washington, DC.

The subcommittees met, pursuant to notice, at 2:18 p.m., in Room 2322 of the Rayburn House Office Building, Hon. Fred Upton [Chairman of the Subcommittee on Telecommunications and the Internet] presiding.

Members Present: Representatives Upton, Stearns, Shimkus, Terry, Markey, Wynn, Gonzalez, Inslee, Eshoo, Murphy, Green and Dingell (ex officio).

Staff Present: Kelly Cole, Counsel; Howard Waltzman, Chief Counsel, Telecommunications and the Internet; Chris Leahy, Policy Coordinator; Brian McCullough, Professional Staff Member; Billy Harvard, Legislative Clerk; Anh Nguyen, Legislative Clerk; Johanna Shelton, Minority Counsel; and Alec Gerlach, Minority Research and Press Assistant.

MR. UPTON. Good afternoon. Today, the Subcommittee on Telecommunications and the Internet, in conjunction with the Subcommittee on Commerce, Trade, and Consumer Protection, chaired by Mr. Stearns, will examine, ICANN Internet governance: Is it working?

I would like to note that, on a cold February afternoon in 2001, I convened my first hearing as Chairman of the Telecommunications Subcommittee. And the subject that day was ICANN, the Internet Corporation for Assigned Names and Numbers. The focus that afternoon was protecting our kids on the Internet, and the law creating the new dot kids site with the dot U.S. country code Internet domain was a product of that very first hearing.

While much has changed since February 2001, there continues to remain constants when it comes to ICANN Internet governance, one of which is the Department of Commerce's oversight. Commerce continues to have a role regarding oversight of ICANN, and I am quite pleased to

hear and read that the Memo of Understanding was extended beyond September 30th. I am anxious to hear the terms of that agreement.

As we discuss the issues this afternoon surrounding ICANN, I am particularly interested in details as they relate to some of the complaints. While some believe that the U.N. should assume control of ICANN, there are too many red flags for me to ignore. Although some have complained about the lack of transparency of ICANN, moving its function to the U.N. is no way to fix the problem. In fact, it will likely make it worse.

I look forward to hearing from our witnesses today as they give their thoughts on how to move forward.

Allowing ICANN to continue to develop under the watchful eye of the Department of Commerce is not only the right thing to do but the most prudent action as well. The stakes are too high.

I yield back my time. And I would recognize the Ranking Member of the full committee, the gentleman from the great state of Michigan, Mr. Dingell.

[The prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF THE HON. FRED UPTON, CHAIRMAN, SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET

Good afternoon. Today, the Subcommittee on Telecommunications and the Internet, in conjunction with the Subcommittee on Commerce, Trade and Consumer Protection, will examine "ICANN Internet Governance: Is it Working?"

I would like to note that, on a cold February afternoon in 2001, I convened my first hearing as chairman of the Telecommunications Subcommittee, and the subject of that hearing was ICANN – the Internet Corporation for Assigned Names and Numbers. The focus that afternoon was protecting our kids on the internet, and the law creating the new .kids site within the .us country code internet domain was a product of that very first hearing.

While much has changed since February 2001, there continues to remain constants when it comes to ICANN Internet governance, one of which is Department of Commerce oversight. Commerce continues to have a role regarding oversight of ICANN, and I am quite pleased to hear that the Memo of Understanding was extended beyond September 30th. I am anxious to hear the terms of the agreement.

As we discuss the issues this afternoon surrounding ICANN, I am particularly interested in details as they relate to some of the complaints. While some believe that the UN should assume control of ICANN, there are too many red flags to ignore. Although some have complained about the lack of transparency of ICANN, moving its functions to the United Nations is no way to fix that problem. In fact, it will likely make them worse.

I look forward to hearing from our witnesses today as they give their thoughts on how to move forward.

Allowing ICANN to continue to develop under the watchful eye of the Department of Commerce is not only the right thing to do, but the most prudent action as well. The stakes are too high.

I yield back the balance of my time.

MR. DINGELL. Mr. Chairman, thank you. I commend you and our other colleague, Mr. Stearns, for holding this hearing. I think it is a very important one. It involves the Internet Corporation for Assigned Names and Numbers, and this is something which is critically important to our national and economic security. The Internet is also an important tool for communication and commerce worldwide. It is ICANN's job to assure the many technical--I hope everybody heard that word--technical pieces of the Internet from root servers to domain name registries are coordinated and function smoothly and securely. Therefore, ICANN's actions are a matter of deep concern to many and to this Congress.

ICANN continues to fall short in representing the interests of the broad Internet community. The last time, under your leadership, Mr. Chairman, this committee held a hearing on ICANN more than 5 years ago. Many serious questions were raised at that time. While ICANN has since made some progress in instituting reforms, several fairness, transparency and accountability issues and problems remain. Following the creation of the Internet in the U.S., ICANN was formed in 1998 as a global nongovernmental organization with guiding principles of stability, competition, bottom-up coordination and representation.

The Department of Commerce's relationship with ICANN was under review at last year's United Nations World Summit on the Information Society. With the bipartisan support of this committee and the Congress, attempts to shift Internet control away from the current framework were quelled. The international community instead reached consensus on maintaining a stable and secure Internet and continuing further dialogue on Internet governance. That said, we cannot allow U.S. interests to be put at risk by blindly ignoring ICANN's flaws or failing to seek improvement for fear of global dissatisfaction. Indeed, I would worry that there may perhaps be more risk to us in ignoring than in proceeding to address this matter. As the Department negotiates an extension of the Memorandum of Understanding, further reforms must be sought. And the Memorandum of Understanding must be held up to the light for all to see and understand. ICANN remains far from a model of effective and sustainable self governance. It seems, however, to be a device which has a rich opportunity for prosperity and profit to some. Moreover, the Department should be sensitive that the manner in which the dot com registry contract is renewed bears on the integrity of ICANN and the Department itself.

After a legal dispute between ICANN and VeriSign, they agreed on a new contract to enable VeriSign to continue operation of the dot com registry. ICANN's approval of this new contract has been roundly criticized by stakeholders in the Internet community as anti-competitive and as lacking in fairness, transparency, and accountability. We will

want to know whether those facts are so. It appears that, even though the current contract does not expire until November 2007, ICANN and VeriSign got together off the record and agreed on a mutually beneficial settlement to a legal dispute and then rushed approval of a new dot com contract changing longstanding registry policies without effectively addressing input from the broader Internet community.

I have previously raised questions over the apparent lack of arms-length negotiations between ICANN and VeriSign, and I take little comfort that ICANN has apparently not changed its behavior. The proposed contract is worrisome in part because it would remove the prospect of competitive bidding for the dot com registry--and I think that is an important matter--and the better services and lower prices that could result for the public. This change is particularly troubling since, last year, VeriSign lowered its registration from $6 to $3.50 and implemented other improvements when the dot net registry contract was re-vetted.

We, I think, should be inquiring as to why some benefit of this kind has not transpired with regard to other contracts and perhaps why people were interested in achieving this kind of goal instead of one which gave us more competition. Another problem is that under the dot com contract, which represents by far the largest and most profitable Internet registry, VeriSign would be permitted to raise registration fees by 7 percent in 4 of the next 6 years without the justification of infrastructure investment that occurs today. And I note that one of the things that we see in technical matters and technology is that prices tend to go down when there is competition. We do not see it going down. We see it going up.

The Department must take sufficient time to review fully the implications of this agreement. With years to go before the contract expires, there is no need for haste. ICANN and, ultimately, the Department, must ensure that all registry agreements are made in a fair and open process and that they are fair to all who are concerned. And this must be done with attention to ICANN's core principles. Our constituents may not be familiar with ICANN, but they use domain names every day, and they need and deserve assurance that their government is doing all it can to support a secure and well-governed Internet. They also need to know that this Nation, because of the way we are managing these things, is not losing the support of the international community, a matter of concern to me also today.

I thank our witnesses for coming before us today, and, gentlemen, I look forward to your testimony.

Thank you, Mr. Chairman for your courtesy.

MR. UPTON. Thank you.

I recognize the Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection, Mr. Stearns.

MR. STEARNS. And I thank my colleague and I welcome this opportunity to have this joint hearing between our two subcommittees. I think we have an opportunity to better understand how the safe and secure functioning of the Domain Name System, the DNS, under the watch of ICANN is integral to protecting consumers strengthening the United States economy and providing the Internet security necessary for e-commerce and other sensitive online functions. We all know what the Internet has done since the Telecom Act of 1996, and we see that the Internet has fueled increase productivity here in America.

At home, the Internet has led a tremendous, tremendous economic growth for innovative American and global companies. According to Forrester Research, online retailers achieved over $170 billion in sales during 2005 and expect to make over $300 billion by the year 2010. The annual value of business-to-business transaction is approximately valued at $2 to $3 trillion. So I believe the DNS system administered by ICANN, with very significant private sector involvement, has been, as my colleagues have pointed out, a total success.

Restructuring this arrangement--one that has obviously worked well over many years--could very well lead to greater uncertainty, less innovation, and fewer choices for consumers. The Internet is built upon the flexibility to develop from the bottom up, rather than from governmental mandates. But despite the success of the Internet under this model and under ICANN since 1998, some governments around the world would like to see some changes. Specifically, some would like to see it put under the U.N. agency. The fact is, of course, that the United States invented, developed and shared the Internet with the world. Heavy-handed government involvement, particularly by supra-national institutions like the United Nations, I think, would spell disaster for a system that is thriving around the world. Politics and policy agendas have no place in the ICANN system and in the operation of the DNS. I will oppose any efforts for a number of reasons to put it under the U.N. jurisdiction. The Internet is just too important for the positive economic and social benefits for this country, and second, "if it is not broke, don't fix it." The current structure has been successful and works.

On another issue that I would like to discuss with my colleagues, through our subcommittee, is the tangential effect any changes could have on the prevalence of online fraud and general consumer protection, as well as the less obvious security issues that would most certainly develop if we start making wholesale changes to ICANN and the way the DNS is administered. My subcommittee has had hearings. We have looked at a number of issues through the Federal Trade Commission.

They have the jurisdiction of enforcing these. What is clear is that the Internet scams continue to proliferate, and we must continue to try to give the Federal Trade Commission the tools they need to stop these frauds. I want the ICANN governance structure and its technical requirements to help the Federal Trade Commission's ability to combat fraud, not hinder it. Mechanisms that provide information about owners of websites and domain names is one way we are helping fortify the DNS system, and I believe, my colleagues, we need to preserve that. The system is working and is working well. I am not interested in making changes that would in any way endanger what has proven to be one of the most powerful tools in history for empowering American commerce and the American consumers. And I would like to thank our witnesses today for attending and their participation. Thank you.

[The prepared statement of Hon. Cliff Stearns follows:]

PREPARED STATEMENT OF THE HON. CLIFF STEARNS, CHAIRMAN, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

Good afternoon. I'm very pleased that we have an opportunity to understand better how the safe and secure functioning on the Domain Name System (DNS) under the watch of ICANN is integral to protecting consumers, strengthening the U.S. economy, and providing the Internet security necessary for e-commerce and other sensitive on-line functions. The economic might of the Internet is everywhere. It is has been adopted by both the titans of global commerce and the local main street store in the smallest towns in America. The Internet has fueled an increase in productivity worldwide, but has also provided positive economic and social benefits to many parts of the world that previously had limited contact with the global marketplace. At home, the Internet has led to tremendous economic growth for innovative American and global companies and has given consumers powerful new tools to stay informed and empowered. According to Forrester Research, online retailers achieved over $170 billion in sales during 2005 and expect to make over $300 billion by 2010. The annual value of business-to business transactions is approximately valued at $2-3 trillion dollars.

I believe the DNS system administered by ICANN, with very significant private sector involvement, has been a success. Restructuring this arrangement – one that has worked well over the years – could very well lead to greater uncertainty, less innovation, and fewer choices for consumers. The Internet is built upon the flexibility to develop from the bottom up, rather than from governmental mandates. But despite the success of the Internet under this model and under ICANN since 1998, some governments around the world would like to see changes. Specifically, some would like to see it put under a U.N. agency. The fact is that the U.S invented, developed and shared the Internet with the world. Heavy-handed government involvement, particularly by supra-national institutions like the United Nations, would spell disaster for a system that is thriving around the world. Politics and policy agendas have no place in the ICANN system and in the operation of the DNS. I WILL OPPOSE any such efforts for a number of reasons. First, the Internet is too important for the positive economic and social benefits it has brought the world to be weighed down by a dysfunctional, multi-government bureaucracy. And second, "if it's not broke, don't fix it." The current structure has been success and WORKS! If improvements are required to ICANN and its processes, that is a much easier process than constructing another U.N organization.

Another issue important to the Commerce Trade, and Consumer Protection Committee is the tangential effect any changes could have on the prevalence of on-line fraud and general consumer protection, as well as the less obvious security issues that would most certainly develop if we start making wholesale changes to ICAAN and the way the DNS is administered. My Subcommittee has looked at a number of issues that the FTC is charged with enforcing. What is clear is that Internet scams continue to proliferate, and we must continue to try to give the FTC the tools they need to stop these frauds. I want the ICANN governance structure and its technical requirements to help FTC's ability to combat fraud, not hinder it. Mechanisms that provide information about owners of websites and domain names is one way we are helping fortify the DNS system, and I believe we need to preserve that. The system is working and is working WELL. I am not interested in making changes that would in any way endanger what has proven to be one of the most powerful tools in history for empowering American commerce and the American consumer.

Again, I'd like to thank everyone for joining us this afternoon and I look forward to the testimony of this distinguished panel.

Thank you.

MR. UPTON. Thank you, Mr. Stearns. I would recognize the Ranking Member of the Subcommittee on Telecommunications and the Internet, Mr. Markey, from Massachusetts, for an opening statement.

MR. MARKEY. Thank you, Mr. Chairman.

And thank you to Chairman Stearns as well for calling this hearing today on Internet governance.

ICANN is an organization with international representation that, through an agreement with the United States Department of Commerce, manages a system of Internet domain names. Simply put, ICANN's role is to coordinate the management of the technical elements of the domain name system so that the Internet users the world over can efficiently ensure that there are valid addresses, whether they are the top level domains, dot com, dot org or others. It has been several years since we had an oversight hearing on the NTIA and its handling of the Memorandum of Understanding between the U.S. Government and ICANN.

At the last hearing, it was evident that ICANN was struggling in several areas, including the adequacy and efficiency of its various processes and its responsiveness to the Internet community generally. I think it is fair to say that ICANN has made strides and has improved its operations in many ways. And I want to commend Dr. Paul Twomey for efforts he has made to ensure that ICANN functions in a manner consistent with ICANN's mandate as well as our broader goals for the Internet.

I do not believe that the United Nations or a variation of the same can or should replace ICANN. Having said that, I do not believe that means we ought to simply leave ICANN to its own devices without comment or critique. So while it has improved, I do not believe that

ICANN has finished its task, reformation. For example, I believe that the organization ought to explore additional ways of ensuring that its so-called constituency effectively captures the demographics and uses of the Internet today. This is a challenging task, as the Internet, at its best, is constantly being reinvented.

In addition, I remain concerned that ICANN still lacks an effective means for achieving accountability. Aggrieved parties need some way through some impartial vehicle and through a dispassionate arbiter to register complaints and seek redress if warranted. More challenging is addressing a practical dividing line between what ICANN is tasked to do and what it is not intended to do. Many have lamented that ICANN appears to set policy when it was simply set up to do rather narrow technical issues. In ICANN's defense, some rather narrow technical resolutions can have practical and significant policy implications. As Mitch Kapur, the founder of Lotus, has said, architecture is policy. And to the extent to which ICANN has some role in the technical configuration of the DNS, it is, willing or not, going to affect, directly or indirectly, Internet policy for companies and countries.

The reality is that NTIA must ensure that the Memorandum of Understanding clearly restrains unintended policymaking by ICANN, and NTIA must also be willing to speak up when ICANN transgresses its charter. Otherwise, all we get is high-tech handwringing. And I get to paraphrase Winston Churchill again about ICANN being the worst form of Internet governance except, of course, all other forms.

Finally, as we look forward, the future of ICANN and its ongoing reform, I do have some concerns that the recent agreement with VeriSign has several provisions which evidence tendencies towards a counter-reformation. I would encourage NTIA to very closely examine the provisions of this new contract. First, it appears that the amount and mechanism for determining prices is untethered to any data about actual cost and is itself untethered from commitments to perform functions for which these price increases are ostensibly justified. I am not saying the prices cannot be justified somehow or that the contract cannot be easily amended to correct deficiencies in the apparent latitude of uses for which this additional revenue may be used. All I am saying is that they are not now. And parenthetically, saying that these price caps were run by the Bush Administration's antitrust division is like saying that they checked with Rip Van Winkle, because that division has suffered a 5-year bout of bureaucratic narcolepsy. In short, the historic sound of its marketplace-protecting bark has been drowned out by the hum of its snoring. So there is little comfort in any such consultation.

Finally, we have spent considerable time here and in the Homeland Security Committee debating terrorism and cyber security. In the

pending ICANN-VeriSign contract, there is no baseline for oversight for monitoring and mitigating ongoing security risks to the DNS. ICANN should modify this agreement to ensure that operators provide detailed security plans and safeguards for the DNS. ICANN would do well to develop independent means of assessing vulnerabilities so that these can be addressed in future agreements as necessary. These economic security and national security shortcomings are ones that NTIA clearly has an opportunity and an obligation to address. Again, I want to thank the chairmen for your hearing today. And I yield back the balance of my time.

MR. UPTON. Thank you.

The gentleman from Illinois, Mr. Shimkus.

MR. SHIMKUS. Thank you Mr. Chairman. Thank you for this hearing. We all know the history of ICANN and this issue of memorandums of understanding and the domain debate. A few of us have dealt with ICANN personally, and I am glad to see my friend, Mr. Markey, here, because, as a new member, when we started doing our dot kids debate dealing with ICANN, we found ICANN to be everything frustrating that it advertised itself to be; not transparent, not open, but confusing, frustrating. So that is why, when we are in this time of this extension of this Memorandum of Understanding, having not seen any real reforms based upon our previous, our last dealings with ICANN, you know, I really would hope that the NTIA would really go to work and help us believe that there is a process here by which the public as a whole can have some light of day. I mean, the public demands from politicians that the light of day be shown on our activities. And we move to do that through campaign finance reform, through public debate, through all sorts of issues. There is no reason why this ICANN cannot be more open, more accessible, more visible.

And I think we have failed. And that is why the importance of this hearing here is to ask these questions in which we will--I will do it when I get a chance to get into my line of questioning, sole proprietorship. The ability to affect the lives of the Internet system is not acceptable without scrutiny. Having the ability to have it--we still want it under the NTIA. We want to make sure it stays within the purview of a trusted international country like the United States so we know that there is safety and security. With what has gone on at the U.N. the last couple of days, the last thing we would want is any movement in an international community. Could you imagine the farce and the jokes that that would create of the World Web and the Domain Names System? So thank you, Mr. Chairman. I hope to learn a lot from this hearing. I yield back.

MR. UPTON. Mr. Gonzalez.

MR. GONZALEZ. Waive opening.

MR. UPTON. Mr. Wynn.

Ms. Eshoo.

MS. ESHOO. Thank you, Mr. Chairman, for holding this hearing. I think it is an important one. And it is a subject matter that hasn't been visited by the committee for a number of years. In fact, I think it was February 2001, and it was your first hearing as a subcommittee chairman. So I welcome it.

I think that there are issues to examine here, and I think that it is an opportune time to say that ICANN, like any new organization, always has to go through growing pains. And since it was created 8 years ago, you have certainly had yours and been a frequent target of criticism among the Internet global community. Some of the criticisms, I think, are legitimate, and they are appropriate. And I think that ICANN still continues to struggle to exercise appropriate and thorough oversight over the technical and administrative functions under its jurisdiction. I think ICANN and consumers would benefit enormously from more transparency. Maybe it isn't written anywhere in the agreement or in the directive that says you don't have to speak to anyone, but, you know what, it is not such a good way to operate.

And so I think that transparency should be taken seriously by the organization and that you take some really solid steps to bring about transparency and broader input, as Mr. Markey said, from the Internet constituents. That would go a long, long way, and it is beyond me why that doesn't happen, but you know, in life, when you don't talk to someone, it is the first sign of something not being healthy. So I wanted to touch on that.

Of course, you were founded in response to growing concerns about U.S. domination of the Internet, and I think today still many countries believe that the United States continues to exert undue influence over the organization and the administrative functions of the Internet. I think that it is important to note that you have enjoyed several noteworthy accomplishments. You have successfully introduced competition to both the retail and the wholesale domain name business and both of those were former monopolies. So that is a big transition. Driven down prices in the domain name market worldwide.

I think it is also important to note that, under ICANN's tenure as the manager of the Internet, that domain names have coincided with an explosion of Internet usage. Today, more than 1 billion users worldwide rely on the Internet. And that is absolutely extraordinary. That is a 300 percent increase since 2001, almost a 300 percent increase since you became subcommittee chairman.

It is now estimated that 25 percent of America's economic value moves over network connections each day. That is quite extraordinary. I

think that ICANN and the domain name service providers it manages have been successful in defending the system from security threats and kept the system up and running. The most important and heavily trafficked domains, the dot com and the dot net, are operated by VeriSign, whom you are very familiar with, and they are a company headquartered in my district in Mountain View, California. And they have maintained 100 percent up time for dot com, and it has never failed.

I have heard from people on the management of these issues. Again, I think that transparency is something that's really needed--more transparency brought to the process.

So we have a lot of catch up in talking to you today because we haven't done that for a long time. So, Mr. Chairman, I am glad that you are having the hearing. I hope that in the next Congress and future congresses, that we won't wait as long to come back to this. This is an area that is growing in leaps and bounds, and I think that our oversight and our interest in it needs to be brought more into play with all the stakeholders that are a part of it. So I am glad you are here. Thank you for having the hearing. I will look forward to talking to you and asking some questions.

[Additional statements submitted for the record follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman, for holding this joint subcommittee hearing on the Internet Corporation for Assigned Names and Numbers, otherwise known as ICANN. ICANN is one of the "behind-the-scenes" organizations that help run the Internet. More specifically, ICANN is responsible for the addressing and naming functions of the Internet to ensure universal resolvability – which simply means that when I type an address into my browser, like www.house.gov, that I actually get to the website I want.

It's been five years since this Committee's last hearing on ICANN, and much has changed since 2001. Five years ago, this Committee was inundated with complaints about how ICANN was run, what its mission should be, and its unresponsiveness. And while complaints about accountability and transparency have not disappeared, we have before us today a much-improved ICANN that is capable of managing the technical functions it has been assigned.

But I do not believe that it is time to eliminate the Commerce Department's oversight role in ICANN. ICANN has some work to do before I would be comfortable asking the Department of Commerce to permit ICANN to be totally independent.

Even with its deficiencies, however, ICANN offers a far better model to achieve transparency and administrative fairness than the U.N. Private sector leadership has enabled the Internet to evolve into the great medium it is today. Given the Internet's importance to the U.S. economy as well as the global economy, it is essential that the underlying domain name system of the Internet remains stable and secure. While the attempt to give these functions to the United Nations failed earlier this year, I do not expect this debate to disappear. But I will continue to oppose this idea – there is little the United Nations can do that private industry can't do better.

I look forward to the testimony of our witnesses and thank you for holding this hearing.

MR. UPTON. Thank you.

I want to thank our panel for submitting their testimony early. I will tell you that it is part of the record in its entirety. At this point, we are going to ask you to summarize your testimony and not to exceed 5 minutes. I believe there is as a clock in the front. I think it is behind Mr. DelBianco. When the red light goes on, that means the 5 minutes has expired. And we will try to do the same for members. I will ask unanimous consent that all members have the opportunity to put their statements in as part of the record at the beginning.

We are joined by Mr. John Kneuer, Acting Assistant Secretary for Communications and Information, from the United States Department of Commerce; Mr. Paul Twomey, President and CEO of Internet Corporation for Assigned Names and Numbers, ICANN; Mr. Steve DelBianco, Vice President for Public Policy from the Association for Competitive Technology on behalf of NetChoice Coalition; Mr. Thomas Lenard, Senior VP for Research from the Progress & Freedom Foundation; Mr. Harold Feld, Senior VP for the Media Access Project; and Mr. Mark Bohannon, General Counsel and Senior VP of Public Policy for the Software & Information Industry Association.

STATEMENTS OF JOHN M. R. KNEUER, ACTING ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, UNITED STATES DEPARTMENT OF COMMERCE; PAUL TWOMEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS; STEVE DELBIANCO, VICE PRESIDENT FOR RESEARCH, THE PROGRESS & FREEDOM FOUNDATION; HAROLD FELD, SENIOR VICE PRESIDENT, MEDIA ACCESS PROJECT; AND MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, PUBLIC POLICY, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

MR. UPTON. Gentlemen, we are delighted that you are here.

Mr. Kneuer, we will start with you. Welcome.

MR. KNEUER. Thank you.

Chairman Upton, Chairman Stearns, members of the committee, my name is John Kneuer. Thank you for this opportunity to testify before the committee on the progress of ICANN meeting its obligations under its Memorandum of Understanding with the Department of Commerce. The department continues to believe that the stability and security of the

Internet and Domain Name System can best be achieved by transitioning to the private sector. The vehicle for that transition has been ICANN and the memorandum of understanding that it has with the Department of Commerce.

This Memorandum of Understanding does not establish a relationship of regulator and regulated between the department and ICANN; rather it is a vehicle for our cooperation and participation in achieving this transition in an efficient manner. Under the terms of the MOU, we offer our expertise and advice on the transition, and we monitor ICANN's performance under the MOU.

The current MOU was drafted to permit the department and ICANN to measure progress towards concrete goals and objectives. When the current MOU was entered into in 2003, ICANN had just completed its own internal review of its processes and was well into the process of implementing structural and organizational changes. That MOU, the most current MOU, is intended to provide a vehicle and a tool for measuring their progress and making those reforms.

The current MOU expires on September 30th of this year. In preparation for that expiration and examining what the path forward would be, at NTIA, we undertook a public consultation this summer. We issued a notice of inquiry, held public meetings. We received more than 700 comments from interested parties around the world, from governments, nongovernmental entities, registrars, registries, pretty much the entire cross-section of interested stakeholders in the Internet. The majority of these stakeholders continue to endorse the original principles put forward in the MOU and those that guided DNS transition, stability and security, competition, bottom-up policy coordination and broad representation. More importantly, the consultation revealed strong support for more specific focus on transparency and accountability for ICANN, the continued involvement of the Department of Commerce in helping with this transition.

As we approach the end of this term of the MOU, we are working with ICANN, and we are negotiating an extension of the MOU. In conclusion, we continue to be supportive of private-sector leadership in the coordination of the technical functions related to the management with DNS. Furthermore, we continue to support the work of ICANN as the appropriate coordinator of these technical functions. Both ICANN and the department agree that preserving security and stability of the Internet DNS is a critical priority that will guide our work in the next stage of the transition. Thank you, and I will look forward to any of your questions.

[The prepared statement of John M. R. Kneuer follows:]

PREPARED STATEMENT OF JOHN M. R. KNEUER, ACTING SECRETARY FOR COMMUNICATIONS AND INFORMATION, UNITED STATES DEPARTMENT OF COMMERCE

Mr. Chairman,

Thank you and the members of the Committee for this opportunity to testify on the progress of the Internet Corporation for Assigned Names and Numbers (ICANN) under the Memorandum of Understanding (MOU) between ICANN and the Department.

The Administration recognizes the critical importance of the Internet to the economic and social well-being of the United States and the global community, and is committed to its future growth. The Department has been charged with preserving the stability and security of the Internet's underlying infrastructure - the domain name and addressing system. I am pleased to have this opportunity to share the results of our efforts to date, as well as our perspective for the future.

The Department's Relationship with ICANN

The Department continues to believe that the stability and security of the Internet domain name and addressing system (DNS) can best be achieved by transitioning the coordination of the technical functions related to the management of the DNS to the private sector. The vehicle for achieving this goal is the MOU between the Department and ICANN. As the Committee will recall, ICANN was formed in 1998 in response to the Department of Commerce's call for a partner to lead the transition to private sector management of the DNS.

In September, 2003, the Department and ICANN agreed to renew the MOU for a period of three years, with several date-specific milestones and broad tasks aimed at guiding ICANN to a stable, independent, and sustainable organization. The expectation of the Department was that the three-year time frame would allow ICANN sufficient opportunity to formalize appropriate relationships with the organizations that form the technical underpinnings of the Internet, secure the necessary resources to ensure its long-term independence, improve its mechanisms for broad participation by all Internet stakeholders, and continue to improve its decision-making processes. The Department plays no role in the internal governance or day-to-day operations of the organization. However, under the terms of the MOU, the Department monitors and ensures that ICANN performs the MOU tasks, and offers expertise and advice on certain discrete issues.

As you may recall, this relationship was the focus of much debate at last year's United Nations World Summit on the Information Society. To provide clarity to this debate, the Administration issued the *U.S. Principles on the Internet's Domain Name and Addressing System*. In this set of principles, the Administration reiterated its commitment to preserving the security and stability of the Internet domain name and addressing system; recognized that governments have legitimate public policy and sovereignty concerns with respect to the management of their country code top level domains; reaffirmed its support for ICANN; and encouraged continued dialogue on Internet governance issues. After much discussion and debate, and with your help and support, the international community arrived at a consensus on the importance of maintaining the stability and security of the Internet, the effectiveness of existing Internet governance arrangements, and the importance of the private sector in day-to-day operations of the Internet.

Measuring Progress

The current MOU was deliberately crafted to permit the Department and ICANN to measure progress toward discrete goals and objectives. When this MOU was entered into in September, 2003, ICANN had just completed an internal review and reform effort, and was well into the process of implementing the structural and organizational changes

called for through that process. In the course of the past three years, ICANN has successfully met many of the MOU's date-specific milestones, which included the following:

- developing a strategic plan addressing administrative, financial and operational objectives;
- developing a contingency plan to ensure continuity of operations in the event ICANN incurs a severe disruption of such operations, by reason of bankruptcy, corporate dissolution, natural disaster or other financial, physical or operational event;
- conducting a review of corporate administrative and personnel requirements and corporate responsibility mechanisms;
- developing a financial strategy to secure more predictable and sustainable sources of revenue;
- improving its processes and procedures for the timely development and adoption of policies related to the technical management of the DNS;
- implementing reconsideration and review processes, including an Ombudsman and commercial arbitration clauses in ICANN contracts;
- developing a strategy for the introduction of new generic top level domains, including internationalized domain names;
- enhancing broader participation in ICANN processes by the global community through improved outreach, regional liaisons, and multilingual communications;
- publishing annual reports on community experiences with the WHOIS Data Problem Reports System, used to report inaccuracies in the submission of WHOIS data by domain name registrants; and
- publishing annual reports on the implementation of the WHOIS Data Reminder Policy, which domain name registrars are required to send to domain name registrants.

ICANN has also made steady progress toward the MOU's broader tasks, including: entering into an agreement with the Regional Internet Registries to facilitate the development of global addressing policy, and developing and implementing new accountability framework agreements with many country code top level domain operators.

Future Relationship

The current MOU expires on September 30, 2006. Over the course of the past year, the Department has conducted an internal review of its relationship with ICANN. To complement the Department's internal review of ICANN's progress under the MOU, the National Telecommunications and Information Administration (NTIA) initiated a public consultation process to obtain the views of all interested stakeholders. In May, 2006, NTIA issued a *Notice of Inquiry on the Continued Transition of the Technical Coordination and Management of the Internet Domain Name and Addressing System* to solicit views on such issues as:

- ICANN's progress in completing the core tasks and milestones contained in the current MOU, and whether these activities are sufficient for transition to private sector DNS management by the scheduled expiration date of the MOU, of September 30, 2006;
- Whether the principles underlying ICANN's core mission (i.e. stability, competition, representation, bottom-up coordination and transparency) remain relevant and whether additional principles should be considered;

- Determining whether the tasks and milestones contained in the current MOU remain relevant, and/or whether new tasks would be necessary;
- Assessing whether all key stakeholders are effectively represented and involved in ICANN's activities, and if not, how that could be accomplished; and
- Whether new methods or processes should be considered to encourage greater efficiency and responsiveness.

NTIA received and analyzed over 700 responses from individuals, private corporations, trade associations, non-governmental entities, and foreign governments. NTIA invited a representative sample of these interested stakeholders to participate in a public meeting on July 26, 2006. Representatives from the Regional Internet Registries, the root server operators, registrars, registries, country code top level domain operators, the Internet Society, the Internet research and development community, trademark interests, the user community, the business community, and a representative from the Canadian government shared their perspectives on the questions NTIA posed to the global Internet community. Well over one hundred interested stakeholders participated in the public meeting.

This public consultation process revealed broad support for continuing the transition the coordination of the technical functions related to the management of the DNS to the private sector through the continued partnership between the Department and ICANN. A majority of interested stakeholders continue to endorse the original principles put forward to guide the DNS transition – stability and security; competition; bottom-up policy coordination; and broad representation. Equally importantly, the consultation process revealed strong support for a more specific focus on transparency and accountability in ICANN's internal procedures and decision-making processes, and the continued involvement of the Department of Commerce in this transition.

As we approach the end of this term of the MOU, we are working with ICANN to negotiate the next phase of our continued partnership.

Conclusion

In conclusion, the Department continues to be supportive of private sector leadership in the coordination of the technical functions related to the management of the DNS as envisioned in the ICANN model. Furthermore, the Department continues to support the work of ICANN as the coordinator for the technical functions related to the management of the Internet DNS. Both ICANN and the Department agree that preserving the security and stability of the Internet DNS is a critical priority that will guide/govern the next stage in the transition process.

Thank you and I would be happy to answer any questions that you may have.

MR. UPTON. Thank you.

Dr. Twomey.

DR. TWOMEY. Thank you, Chairman Upton.

Thank you, Chairman Stearns.

And thank you, members of both committees for the opportunity to speak to you today in my role as President and CEO of ICANN. I feel, after all the members' statements, I should simply stop. I think you have so much knowledge of the organization.

But the best I could say, you know, ICANN has been recognized by the world community as the global authoritative body on the technical

and organizational means to ensure the stability and interoperability of the DNS and the distribution of unique identifiers for the Internet, in particular IP addresses.

Since appearing last before Congress, which was nearly 2 years ago in the other place, ICANN has continued to secure a stable and secure Internet that ensures universal resolvability. ICANN has fostered greater choice, lower costs and better services to DNS registrants, including over 10 million businesses in the United States alone. ICANN's successful coordination of its community underpins the operation of the global Internet.

Each day, the system supports an estimated 30 billion resolutions, nearly 10 times the number of phone calls in North America each day. And as members have already pointed out, nearly $2 trillion of e-commerce a year flows across this network. Why is universal resolvability important? Success means that Internet addresses resolve in the same way for every one of the Internet's global users, every one of the one billion people who use the Internet online.

As part of the international private-sector entities tasked to provide technical coordination of the domain system, ICANN in recent years has recognized six new agreements for gTLD registry operations and has finalized negotiations and is waiting for approval of five others. All of the pending agreements have set out language with a greater accountability to ICANN on security and stability concerns and also provide greater opportunity for ICANN to act in the event of actions of registries or such other issues that might arise from registry operator practices.

I might point out to members that all of these agreements have been sent out in an open and consultative process. The new general framework for these contracts was first released publicly 18 months ago and has been discussed over this time, including in four global meetings, and has received several thousand public consultation receipts. To give you a specific example, the dot com agreement is part of a larger, overall settlement of a longstanding dispute with VeriSign over its desire to introduce new registry services. We engaged in a 4-month public process, which included two different public comment periods, the receipt of over 600 public comments and the substantial renegotiation of key terms important to our community. We look forward to the Department of Commerce approving the agreement as provided for in the specifics. New registry agreements have already benefited the Internet community by creating a better working relationship between ICANN and key registry operators, perhaps turning to the relationship with the United States Government. ICANN has been engaged in a longstanding and important relationship with the United States Government.

ICANN is about to successfully complete the sixth separate amendment to the original Memorandum of Understanding with the DOC. And as Mr. Kneuer pointed out, ICANN and the DOC are in conversation about the steps forward. ICANN has recently entered into a new 5-year arrangement for ICANN to manage the Internet address naming authority function. ICANN and the NTIA are in final stages of discussions which will confirm an appropriate continuing relationship and will recognize ICANN's global private sector role and continue the transition of the coordination of technical functions and the management of the DNS to the private-sector. One of the greatest achievements of ICANN has been the successful creation, support, and coordination of an ICANN community and the creation of the bottom-up policy, making process supported by various stakeholders involved in the DNS. The evolution of this model continues in many ways but most recently in the following actions. This week the ICANN board has commenced a review of its own guiding principles and is publishing soon a set of private-sector management operating principles, which will be offered for public review and will be directed, in many respects, to some of the issues raised by members.

Last week, the London School of Economics provided the ICANN commission an independent third-party review of one of ICANN's key policy development supporting organizations, ICANN's generic name supporting organization. The information contained in this review will likely result in considerations of additional improvements to ICANN's GNSO and supporting organizational structures. The key point to point out here is ongoing evolution and ongoing listening to the community about the need to evolve as an organization, both to evolve concerning constituencies and evolve concerning processes and evolve concerning principles for the operation of the organization.

I might just finish with perhaps three--two comments concerning, I think, real achievements of ICANN to address some of the issues members may have heard about and one final comment about transparency and accountability. ICANN has been very concerned to ensure the protection of intellectual property when it comes to domain names, and ICANN's uniform domain name dispute resolution policy has been highly successful and a great barrier to individuals, businesses, and intellectual property holders. The policy allows them to assert their rights against domain name squatters and infringers of intellectual property interests. The UDRP has resolved more than 17,000 disputes over the rights of domain names and has proven to be efficient and cost effective for those utilizing this alternative dispute resolution mechanism.

The market for generic top-level domains has also very much been benefited by the introduction of competition in that space, both the introduction of new gTLDs and the introduction of much increased numbers of generic registrars. When ICANN started its work, there was one registrar, one person who sold domain names. Consumers today can choose from 845 ICANN accredited registrars, derived from more than 250 unique businesses in over 40 countries. And the average cost or the price of domain names saying dot com have now been reduced by as much as 90 percent to consumers.

My final comment on transparency and accountability: ICANN does have well-established principles and processes for accountability in its decision-making and in its bylaws. In particular, after its decision-making processes at the board level, there is the ability for appeal to a review committee, and then, from there, to an independent review panel and independent arbitration. It is interesting to note that none of the ICANN constituencies or members have yet decided to take advantage--to complete an independent review panel or arbitration process. That may actually tell you something about the nature of the accountability of the organization, that, in any of its decisions, nobody has yet decided to use the final method of accountability available to them under the bylaws.

My final observation with regard to the discussion is that there is, I think, quite a bit of distinction between the issue of transparency and the issue of accessibility. ICANN is actually an incredibly transparent organization. It is. If you look on its website, you will find vast amounts of information about the processing and activities underway. Although, I fear it is transparent in a way which certainly is pertinent, I think, at the moment, it is transparent in the way, the same way that credit card agreements are transparent. They are all there; it is just very hard to understand it. And so I think one of the challenges we certainly have is about making our information much more accessible and making certain we do put in place principles that really do address some of the issues of transparency that people have been discussing.

Thank you, Mr. Chairman.

[The prepared statement of Dr. Paul Twomey follows:]

PREPARED STATEMENT OF DR. PAUL TWOMEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

Introduction

Good Morning, Chairman Upton, Chairman Stearns and members of the Committee. Thank you for the opportunity to speak before this Subcommittee in my role as President and CEO of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a private sector organization performing a global function, with our main office in Marina del Rey, California. ICANN has been recognized by the world

community as the global authoritative body on the technical and organizational means to ensure the stability and interoperability of the DNS, and the distribution of IP addresses.

ICANN's Role in Internet Governance

Since appearing before Congress nearly two years ago, ICANN has continued to take great steps forward in solidifying its role as the international private sector entity tasked to provide technical coordination of the domain name system (DNS).

The limited and distinct mission of The Internet Corporation for Assigned Names and Numbers is clearly set out in Article I of ICANN's Bylaws. ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
    a. Domain names (forming a system referred to as "DNS");
    b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and
    c. Protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately as they relate to these technical functions.

Since its origins in 1998, ICANN has helped secure a stable and secure Internet that creates a presumption of universal resolvability. ICANN has fostered greater choice, lower costs and better services to DNS registrants, including over ten million businesses in the United States alone. The Internet requires a stable and secure system of unique identifiers if it is to serve the global community efficiently and reliably.

At the core of ICANN's mission is global interoperability of a single Internet. ICANN was established to serve the Internet community by maintaining the stability and security of the Internet's unique identifier systems, and fostering competition where appropriate to give Internet users greater choice at optimal cost.

ICANN's successful coordination of its community underpins the operation of the global Internet. Each day this system supports an estimated 30 billion resolutions, nearly 10 times the number of phone calls in North America per day. There are currently more than one billion users of the Internet. Due to the universal DNS resolvability secured and coordinated by ICANN, the Internet addresses resolve in the same way for every one of the Internet's global users once online.

ICANN has entered into six new agreements with gTLD registry operators (including .NET, .TRAVEL, .CAT, .JOBS, .MOBI, and .TEL) in the last two years (and has finalized negotiations and is waiting for approval of 5 others). All of the pending agreements have set out language with a greater accountability to ICANN on security and stability concerns, and also provide greater opportunities for ICANN to act in the event of actions of registries, or such other issues that might arise from registry operator actions or practices., including: a) the .COM agreement (which is currently pending approval by the US Department of Commerce) and b) four other registry agreements for .ASIA, .BIZ, .INFO and .ORG (which are subject to review by the ICANN Board of Directors during the next ICANN Board Meeting).

The .COM agreement is part of a larger overall settlement of a long-standing dispute with VeriSign over its desire to introduce new registry services. That dispute arose with the creation of ICANN and has been resolved in a way that would enhance the performance of both entities, to the benefit of all of the users of the Internet. ICANN and VeriSign Board's have both approved settlement documents that would permit the parties to act together in a concerted way to protect the overall security and stability of the Internet. Further, if VeriSign were ever to act in a manner that is inconsistent with the interests of the Internet community, ICANN has built additional mechanisms into the agreement to resolve such disputes promptly and effectively.

Continuing Relationship with the United States Government

ICANN has been engaged in a long-standing and important relationship with the United States Government since ICANN's inception, which has been administered by the US Department of Commerce's NTIA. ICANN is about to successfully complete the sixth separate amendment to its original Memorandum of Understanding with the DOC.

ICANN will continue in its relationship with the United States Government, having recently entered into a new 5-year arrangement for ICANN to manage the Internet Assigned Numbers Authority (IANA) function. Additionally, ICANN and the NTIA are in the final stages of discussions, which will confirm an appropriate continuing relationship and will recognize ICANN's global private sector role providing technical management of the DNS in a manner that promotes stability and security, competition, coordination, and representation.

ICANN's Private Sector Multi-Stakeholder Model and its Continuing Evolution

One of the greatest achievements of ICANN has been the successful creation, support and coordination of an ICANN Community and creation of the bottom-up policy making process supported by various stakeholders involved in the DNS. Since ICANN's creation, the Internet community stakeholders, have vigorously discussed and reviewed ICANN's mission and values. Accordingly, ICANN has continued to build into a robust entity, and has continued to evolve ICANN's multi-stakeholder model, which remains encapsulated in ICANN's Bylaws and its Mission and Core Values.

The evolution continues in many ways, but most recently in the following actions:

1) This week, the ICANN Board, having reviewed the comments about ICANN and its processes generated from the community during the past year, has commenced a review of its own guiding principles and is publishing a set of Private Sector Management Operating Principles (ICANN PSMOPs), which will be offered for public review.

2) Last week, the London School of Economics provided an ICANN-commissioned independent third-party review of one of ICANN's key policy development supporting organizations, ICANN's Generic Name Supporting Organization (GNSO). The information contained in this review will likely result in considerations of additional improvements to ICANN's GNSO and supporting organizational structure.

ICANN's Continuing Accomplishments

Since 1998, ICANN's self-governance model has succeeded in addressing stakeholder issues as they have appeared, and bringing lower costs and better services to DNS registrants and everyday users of the Internet.

ICANN has been continuing its efforts to manage and adapt in the face of continued and dynamic growth of the Internet. ICANN, with the efforts of the ICANN Security and Stability Advisory Committee, has worked to make the Domain Name System more resistant to external attack.

ICANN has undertaken significant work in relation to Internationalized Domain Names (IDNs) that will enable people across the world to interact with the Internet's domain name system in their own languages, which will work to avoid the creation of alternate root systems. Working in coordination with the appropriate technical communities and stakeholders, ICANN's adopted guidelines have opened the way for domain registration in hundreds of the world's languages.

ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) has been highly successful and of great value to individuals, businesses and intellectual property holders. The policy enables them to assert in allowing them to assert their rights against domain name squatters and infringers of intellectual property interests. The UDRP has resolved more than 17,000 disputes over the rights to domain names, and proven to be

efficient and cost effective for those utilizing this alternative dispute resolution mechanism.

After significant study and discussion, and working with the accredited gTLD registrars, ICANN developed a domain name transfer policy enabling domain name holders to transfer management of their domain name from one registrar to another readily. The implementation of this policy has been highly successful and has been an important step in providing additional registrar market changes and greater choice to consumers.

ICANN continues to introduce new Top Level Domains to give registrants right of choice. These include the introduction of seven new gTLDs in 2000 and four additional ones so far from the 2004 sponsored top-level domain name round.

ICANN re-bid the .NET registry during 2005, resulting in a new agreement being executed between ICANN and VeriSign. ICANN has proposed five additional gTLD agreements with the registry operators of .ASIA, .BIZ, .COM, .INFO, and .ORG. All of the newly proposed registry agreements contain new language supporting ICANN's role in the security and stability of the DNS.

The market competition for generic Top Level Domain (gTLD) registrations established by ICANN has lowered domain name costs in some instances by as much as 80 to 90%, with savings for both consumers and businesses. Additional detail is provided below.

Registry-Registrar Level Competition

Since ICANN was founded in 1998, ICANN has entered into many private arms-length agreements with registries (that operate the generic top-level domains), and with registrars (who are accredited by ICANN to sell domain names directly to consumers). Through these actions, ICANN has provided a private-sector solution and helped break down the monopoly position by a single dominant company, which provided both registry and registrar functions to the majority of consumers purchasing domain names.

In 1998, there were only three main generic top-level domain name registries (.COM, .NET, and .ORG) from which domain names could be purchased by American small businesses. Only one company was running all three registries, Network Solutions (which was later acquired by VeriSign). Most registrations by small businesses were in .COM.

There was a single registrar in 1998. That same company that ran the registries, Network Solutions, was the only registrar from which a consumer could purchase a domain name. The price of a single domain name in .COM in 1998, was approximately $90.00 per domain name.

The .COM Registry still controls a significant amount of the marketplace, but now less than 50% of the market, including ccTLD operators.

The price for a .COM registration today depends upon where you purchase the name from, but in some instances the price of a domain name has been reduced by as much as 90%. Today, the price ranges from $7 to $35 per domain name. GoDaddy is now the largest registrar, displacing Network Solutions, which has been spun out of VeriSign.

Consumers can choose from over 845 ICANN-Accredited Registrars, derived from more than 250 unique business groups (a significant number owning interests in multiple registrar companies), located in over 40 countries.

Between 2000 and today, 11 new generic top-level domains have signed agreements with ICANN. Five of those (.CAT, .JOBS, .MOBI, .TEL and .TRAVEL) having signed agreements with ICANN in the last 18 months.

Conclusion

In conclusion Chairman Upton, Chairman Stearns and distinguished subcommittee members, ICANN is committed to its continuing role as the private sector steward of a

stable and globally interoperable Internet, and is committed to fostering competition in the domain name marketplace.

MR. UPTON. Mr. DelBianco.

MR. DELBIANCO. Chairman Upton, members of the committee, NetChoice is a coalition of trade groups, such as the Electronic Retailing Association, e-commerce leaders like AOL, eBay and VeriSign, plus thousands of small e-commerce businesses. They register their own domain names. They build websites, and they do business online.

In my remarks today, I intend only to make three points. The first is that e-commerce really needs availability and integrity from the Domain Name System. Second point, availability has been good, but there is a growing gap on integrity. The third point is to suggest ways that this committee can help close that gap.

The title of today's hearing was with respect to ICANN's Internet governance, but I would suggest to you that ICANN is really the Internet's manager; it is not the governor. And Congresswoman Eshoo called it a manager, the term that you used. The DNS manager actually coordinates, through the use of contracts and agreements, with private-sector entities that have invested $1 trillion to bring the Internet to a billion people around the planet. Now the manager's job in this case is to keep a single interconnected DNS going and growing.

Now, governments, on the other hand, can prosecute crimes, legislate, and they can also regulate content, each in its really own sovereign way. So I am going to agree with some of the opening statements on the committee, as well as some of the panelists here, in suggesting that a multi-governmental body, most specifically the U.N., would make a mess out of DNS management and conclude that we should therefore, wholeheartedly support ICANN's independence from government encroachment.

Now, from our DNS manager, ICANN, America's e-commerce industry really just needs two qualities; we need availability and integrity. Now, availability means being able to get to that website, 24/7, 365, in any language, and even while the Internet domain system is under attack. Integrity, says that when you click on a link, that you actually get to the intended page you were seeking, not redirect yourself to some fraudulent website. And integrity is also meaning that domain names and typographical variance on your domain name should be held by their rightful owner.

Now, DNS availability. The first of those concepts, has been excellent so far; 100 percent up time. But we do need continued investments in infrastructure to maintain availability like that, with growing Internet usage and the growing strategy of attacks.

Now, if I turn to the domain name marketplace, not just the DNS per se, but the marketplace around names, there is a growing integrity gap. And I will just give you three kinds of examples. The Federal Trade Commission and law enforcement in other nations are working to stop phishing, pharming and spam. But I agree with some other witnesses you will hear from today, that ICANN must force registrars to do a better job of maintaining the "Whois" data that is necessary for the FTC to do their job.

Cyber squatting. Another element of integrity has taken on a whole new spin. It is called typo squatting. Some registrars are abusing the 5-day grace period available to them under many registry contracts to learn what are the commonly used typographical errors that users will type in when they enter the name of a website. Now, this has been called domain tasting, but we like to call it sharking. The same way that a shark circles its prey before it decides to attack. Even the largest registrar said yesterday that this sharking is grounds to decertify registrars who conduct it.

Another form is the notion of deceptive content on the websites that are for sale. It used to be that a cyber squatter would display just, oh this name is for sale, contact me to buy it. But now they are a little more creative. Pages themselves are full of links to competitors products. In fact, page 7 of my testimony shows a page for 1800contacts.com, one of my members, and it shows what happens if you type 1-8-o-o instead of 1-8-zero-zero.

The final form of integrity gap I want to point out to you is that registrars are still practicing the slamming technique on domain name owners. That is where a registrar, not the one you initially used, sends you a fraudulent invoice for your domain name renewal months ahead of expiration. If you fall for it, the slammer basically takes over your domain account. In 2003, the FTC prosecuted and obtained a consent decree against a few registrars for slamming, but it still goes on today, and ICANN hasn't aggressively enough decertified, in fact, they haven't decertified a single registrar yet.

Let me close by suggesting three ways the committee can really help to ensure availability and close the gap. First, I think the U.S. Government should continue its oversight of ICANN, adding milestones to enforce contracts and decertify registrars who don't follow the rules. Second, we should select responsible and experienced vendors to run DNS infrastructure and then provide incentives for them to invest in scale and security. And finally, we hope that the FTC would aggressively pursue registrars who slam and any other deceptive practices where they rely upon ICANN to keep the "Whois" data secure. So I thank you and look forward to your questions.

[The prepared statement of Steve DelBianco follows:]

PREPARED STATEMENT OF STEVE DELBIANCO, VICE PRESIDENT FOR PUBLIC POLICY, ASSOCIATION FOR COMPETITION TECHNOLOGY, ON BEHALF OF NETCHOICE COALITION

Chairman Stearns, Chairman Upton, and distinguished members of the Committee: My name is Steve DelBianco, and I would like to thank you for holding this important hearing. I'm pleased to testify on how ICANN's contribution to Internet Governance is working.

I'm the Executive Director of NetChoice, a coalition of trade associations and e-commerce leaders such as AOL, eBay, and VeriSign, plus thousands of small e-commerce retailers.

I also appear before you as a genuine "small business survivor." In 1984 I founded an information technology (IT) consulting firm, and grew it to $20 million in sales and 200 employees before selling the business to a national firm. After that experience, I was drawn to Washington to help start a trade association that focused on the needs of small IT businesses like mine.

In the states, here in Washington, and as a member of ICANN's Business Constituency, NetChoice works to improve the availability and integrity of e-commerce. NetChoice members are growing concerned about threats to trade, security, trademarks, and consumer protection on the Internet. Moreover, we are wary of United Nations and international organizations who covet ICANN's role as manager of the Internet.

The title of today's hearing poses a seemingly simple question—is ICANN Internet Governance working?—though the answer is anything but simple. In my testimony, I will describe current and future concerns and make several recommendations for ICANN and for the U.S. Government in its oversight role. First, however, I should clarify that ICANN's management role is only a part of the overall Internet governance process.

ICANN is the Internet's *Manager*, not its Governor

It's a common perception that ICANN is engaged in Internet governance, but ICANN's stated mission is to ensure the stability and interoperability of the Domain Name System (DNS). It works in coordination with a private sector that has invested a trillion dollars to bring Internet connections to over a billion people around the world. Bearing that in mind, it's better to think of ICANN as the Internet's manager—not its governor.

While ICANN's management focus is commonly described as "security and stability", the Internet community actually relies on ICANN to manage the DNS to achieve two key qualities—***availability and integrity***.

Availability of the DNS is critical for anyone who relies on the Internet for information, communications, and trade. Domain name resolutions need to be available 24 hours a day, 365 days a year, from anywhere on the globe—in any language. Even the slightest degradation or interruption in DNS availability can slow or interrupt access to email and websites.

Integrity of the DNS is vital to both business and end users of the Internet. Businesses rely upon the integrity of domain name registration to ensure that their brands aren't misrepresented or misappropriated. E-commerce and internet financial transactions require integrity in resolution of domain names and secure delivery of encrypted information.

Internet consumers depend upon the integrity of domain name services to provide accurate and authentic results when they lookup a website or send an email. Integrity is undermined by deceptive practices such as redirecting users to fraudulent websites, or providing false information about the true owner of a web domain.

Always-on availability and uncompromised integrity are necessary for a fully functional DNS and a properly performing Internet.

To deliver these qualities, ICANN acts as a project manager, coordinating contracts with vendors and organizations that manage key DNS functions. These contracts and agreements are narrowly tailored and limited in scope to what can be agreed to by consenting parties.

Governments, on the other hand, are public institutions with broad portfolios and the power to compel or punish specific actions. Those powers are an essential part of governing the internet: enforcing trademark laws; protecting consumers from fraud; and prosecuting hackers and criminals.

But imagine if ICANN were run by governments using governmental powers. Quarreling nations would find it impossible to agree on anything but the most trivial technical decisions. Lesser-developed nations would press for changes in Internet management to advance economic development goals. Special interests would seek Internet-enabled social programs to address perceived disadvantages. It's no stretch to imagine a tax, or "contribution," on domain names to fund programs to "bridge the digital divide" and promote local commerce and content.

ICANN Management of the DNS Works (for now)

From the perspective of businesses that rely upon the internet for communications, information, and e-commerce, it's clear that the DNS *is working*. Customers and suppliers can quickly and reliably get to our members' websites, buy online, check the status of an order, or just find the address of the nearest store. Over three-quarters of small businesses say their website generates leads and gives them a competitive advantage.[1] Online retailers realized $172B in sales during 2005 and expect over $300B by 2010, according to Forrester.

The increase in e-commerce has placed greater demand on the DNS. As of June 2006, there were 105 million total domain registrations, and this is 27% more than a year ago.[2] Ten million new domains were registered in the second quarter of 2006, up 33% over the same period in 2005. Compared with 6 years ago, there are four times as many Internet users, and Internet usage is 20 times greater. International Data Corporation estimates that over a billion electronic mailboxes were in use around the world in 2005.[3]

The registry operator for .com and .net domains processed an average of 18 *billion* queries per day in the second quarter of 2006, an increase of 30 percent year-over-year.[4] Moreover, the .com and .net domains have seen 100% uptime reliability for the past 13 years.[5]

Judging by growth and vitality, yes, ICANN's management is working. However, there are several ways that ICANN's management is not working effectively to maintain the most important qualities of the DNS—availability and integrity.

Attacks Threaten Internet Availability & Integrity

Seven major attacks on the DNS availability have occurred in the past six years. The largest attacks on domain name servers hijacked multiple computers to amplify and accelerate the assault. This year, a distributed denial-of-service attack disabled 1,500

---

[1] Source: eMarketer

[2] Domain Name Industry Brief, Vol. 3, Issue 1, August 2006, available at http://www.verisign.com/static/039111.pdf

[3] Background Paper for the OECD Workshop on Spam, Jan. 22, 2004, available at http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF

[4] Id. at Note 2 (Domain Name Industry Brief).

[5] See http://www.verisign.com.sg/dns/comparison.shtml VeriSign manages the DNS for .com and .net.

websites using 32,000 hijacked computers.[6] Symantec estimates that denial-of-service attacks rose 51 percent in the second half of 2005, to an average of 1,400 attacks per day.

Denial-of-service attacks can cripple a website and disable an online business. Moreover, small businesses are experiencing *blackmail* via denial-of-service attacks, where a business owner is forced to pay-up in order to stop the attack.[7]

Attacks on the integrity of the DNS itself are also raising alarms. Attackers can redirect web browsers and DNS servers to fraudulent sites hosting convincing scams. One method of redirection involves corrupting DNS data that's "cached" in memory so that users are pointed to fraudulent websites. Increased security measures can help, but hackers and scam artists are quick to adapt their technology and tactics.

Just how concerned are American businesses by these attacks on the Internet and affronts to consumer protection? To get answers straight from the source, we sponsored a Zogby Interactive poll of 1200 small businesses across the nation, conducted May 26-30, 2006[8]. The poll included questions about Internet availability and the integrity of the domain name system. Top-lines from that poll tell a story in two parts:

- 78% of small biz owners say a less reliable internet would damage their business.
- 78% said reliability & performance were more important than low fees for domain names.
- 68% support a $1.86 hike in domain fees to invest in reliability and security.
- 81% said they are unconcerned about a $1.86 fee increase.

For businesses that rely on the Internet for exposure and for e-commerce, threats to Internet availability are serious concerns. These businesses have little concern about modest price increases for domain names when that money goes towards Internet security and stability.

The second part of the Zogby poll shows that small businesses with websites are questioning the *integrity* of business practices in the domain name marketplace:

- 59% are concerned about cybersquatting—where speculators buy domain names closely related to names of real businesses, and hold them for ransom.
- 69% are concerned about being exploited by registrars who charge exorbitant fees to reinstate a domain name that's been allowed to expire.

The poll findings are unambiguous—the availability and integrity of the domain name system are a concern to business owners. How effective is ICANN in responding to these concerns?

In its new registry operating contracts, ICANN is attentive to security and stability—these exact words appear 26 times in 28 pages of the contract, which also declares ICANN's intention to develop new policies to improve security.

However, ICANN has to react faster to threats and vulnerabilities. After years of study and debate, everything possible should be done to implement DNS security extensions as quickly as feasible. More important, security policies that help ensure availability in the face of tomorrow's threats and vulnerabilities cannot take years to develop and execute. Security delayed is dollars lost and new business opportunities denied.

---

[6] Distributed Denial of Service (DDoS) attacks are conducted by controlling and compromising multiple computers—by the use of "zombies" or "bots"—to send a flood of queries against a targeted website. DDoS attacks generally overload the target's network with a high volume of traffic while simultaneously opening many web pages so that the site runs out of resources to handle legitimate requests. See http://www.symantec.com/avcenter/venc/data/ddos.attacks.html

[7] Daniel Thomas, "Websites face more attacks – BLACKMAIL" *Financial Times*, May 31, 2006.

[8] For the complete Zogby Interactive poll, see www.netchoice.org\ZogbyPoll.htm

Similarly, ICANN has simply taken too long to implement internationalized domain names, a step that would improve Internet availability for populations that don't use the Roman alphabet character set.

An available Internet is one goal of the DNS—the integrity of domain names is another. Unfortunately, the integrity of domain name services is being undermined by unfair and deceptive practices.

An Integrity Gap in the Domain Name Marketplace

The integrity of the DNS is vital to Internet trade and consumer protection. Businesses rely upon the integrity of domain name registration processes for the resolution of domain names and secure exchanges of encrypted information. Internet users depend upon the integrity of domain name services to provide reliable results when sending email and visiting websites. Abusive, fraudulent and unfair practices undermine the integrity that is vital to the DNS.

As manager of the DNS, ICANN can and should do more to assure the system's integrity. Based on its consensus policies, ICANN enters contracts with registries and certifies registrars to manage the availability and integrity of the DNS. Registries contract with ICANN-accredited registrars that resell domain names and provide direct services to domain name owners. These registrars are in the best position to prevent many of the unfair and deceptive practices described below.

Cybersquatting

Cybersquatting is an abusive practice in which a speculator registers a domain name identical or very similar to the trademarked name of a legitimate company or other organization. The speculator can then hold the name for ransom, forcing the trademark owner to pay far more than the actual cost of registration just to get control of a domain name that would not otherwise have any value to anyone.

Cybersquatters unfairly and illegally take advantage of the established value of someone else's trademark. But defending a valuable trademark in court can be prohibitively expensive, especially for a small business. The World Intellectual Property Organization reports year that the number of cybersquatting cases it handled rose 20 percent in 2005.[9]

Under the Anti-Cybersquatting Consumer Protection Act of 1999, trademark owners can sue a cybersquatter or ask ICANN to arbitrate their claim. For a small business, the time and expense needed to understand and assert these legal remedies are often more than the owner can afford. Consequently, most small businesses either continue to lose prospects to cybersquatters, or are forced to meet the ransom demanded.

Typo-Squatting

"Typo-squatting" is registering domain names that closely resemble those of already popular Web sites, usually common misspellings of the legitimate site name.

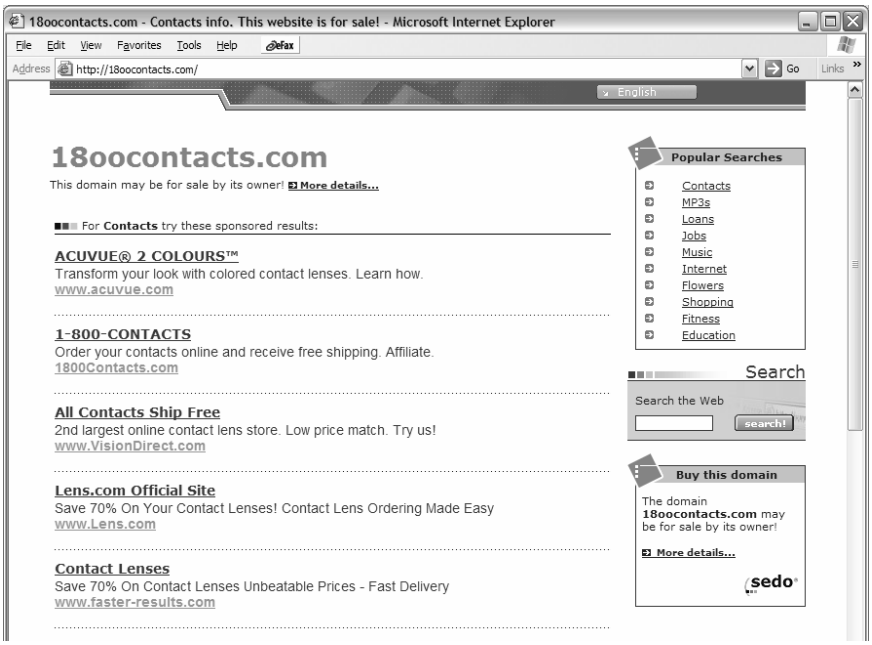
Since almost half of all Web users prefer to type Web site names directly into their browsers, misspellings are inevitable. If a customer accidentally misspells the domain name they are looking for, they can end up instead at a typo-squatter's website. All they find there are advertisements, often for competing products and services.

For example, I tried a few typographical variations on 1800Contacts.com, the leading telephone and online seller of replacement contact lenses, and a NetChoice coalition member. If I enter 18OOcontacts.com instead of 1800contacts.com (letter O instead of numeral zero), I arrive at a page designed to steer me into buying contacts from competing lens sellers. 18OOcontacts.com points to a server owned by Sedo, the current

---

[9] WIPO Responds to Significant Cybersquatting activity in 2005, Press Release 435, January 25, 2006, available at http://www.wipo.int/edocs/prdocs/en/2006/wipo_pr_2006_435.html

leader in "Parking" domain names.[10] Sedo's parking site is designed to generate ad revenue when users who intended to go to 1800Contacts start clicking on sponsored links—*for other lens sellers*. (Screen capture shown below).[11]



When I clicked on the 1800Contacts.com link displayed on this page, I was re-directed to yet another page showing ads for other lens sellers. In other words, *the hyperlink for 1800Contacts.com is falsely labeled in order to generate ad revenue from a competing site*.

Typo-Squatting sites confuse and divert potential customers. 46% of users prefer to type the domain name of a known website directly into the browser's address bar.[12] But when typos happen, legitimate businesses shouldn't lose customers who fall into traps designed to generate ad revenue. What's more, the ad revenue generated by parking drives up the price if the intended business tries to acquire the domain from the parking operator.

The Land Grab on New Top Level Domains

A similar abuse of the domain name registration system, called a "land grab," can occur whenever a new top level domain is launched. Speculators register thousands of names in the new domain, hoping to tie-up names similar to those of legitimate businesses and organizations. The speculators then either ransom these names to their legitimate owner or use them for typo-squatting and ad parking.

For example, when the .eu domain was created for Europe, speculators quickly moved to register names that legitimate businesses and organizations already held on other domains. EUrid, the non-profit organization operating the .eu registry, consequently

---

[10] For information about Sedo, see http://www.sedo.co.uk/about/index.php3?tracked=&partnerid=&language=e

[11] See http://www.18oocontacts.com/

[12] North America Domain Name Study, Windward Directives, June 2005.

suspended 74,000 .eu domain names and sued 400 registrars for breach of contract.[13] A syndicate of registrars had engaged in abusive behavior by warehousing tens of thousands of .eu domain names with the obvious intent of selling them.

Critics of ICANN suggest that the organization exceeds its management role when trying to prevent and resolve domain name abuses. However, ICANN manages policies for initial registration, which is the best point to prevent squatting abuses. And if a trademark dispute arises later, it is far more efficient to use ICANN's arbitration process, saving legal fees and cutting the time to resolve the dispute and re-assign the name.

Registrars are not doing enough to maintain the quality of the "Whois" data needed to fight squatting, fraud, and traffic in copyrighted material and counterfeit goods. ICANN needs to enforce its contracts, and de-certify registrars who fail to meet their contractual obligations to collect, maintain, and display accurate and complete Whois data.

"Sharking" (a.k.a. Domain Tasting)

Domain name "sharking" is an abusive practice in which speculators looking for sites where they can park ads take advantage of the five-day grace period between the time a new domain name is reserved and the time the registration fee must be paid. In April 2006, out of 35 million registrations, only a little more than 2 million were permanent or actually purchased. It's a good bet that a large portion of the other 33 million registrations were part of the sharking scheme.[14]

Speculators routinely register large numbers of potentially attractive domain names and then carefully track how many accidental hits they generate. If a site fails to generate much traffic, the speculator can let the domain name lapse without paying anything. But if the site generates a lot of traffic, the speculator can use it to park ads, often from one of the large managed Web advertising networks like Google, and generate significant revenue with no effort.

ICANN is aware of growing abuse of the 5-day Grace Period policy, and held a workshop in its last meeting in Morocco. Still, I have not seen aggressive moves by ICANN to explore new grace period policies and restrictions to guard the integrity of the DNS from this kind of abuse.

Slamming

Most consumers with a telephone can remember the scourge of slamming – where resellers of long-distance telephone service switched providers only to have the incumbent switch back, and so on. Domain name slamming works in a similar way. A registrar tricks an unwary domain name holder into unintentionally switching from one registrar to another.

Domain name slammers often use direct mail or email spam to target domain name holders with phony renewal notices. If the domain name holder takes the bait, thinking that they are just renewing their subscription with their existing registrar, they may soon be forced to pay whatever the slammer demands or risk losing their domain name when it comes up for renewal.

In the U.S. domain name slamming is a considered an Unfair and Deceptive Trade Practice and has been prosecuted by the Federal Trade Commission. In 2003, one of the largest domain name registrars, Network Solutions, settled a complaint with the Federal

---

[13] *EURid Suspends 74 000 .eu Domain Names*, July 24, 2006, available at http://www.eurid.eu/en/general/news/eurid-suspends-74-000-eu-domain-names-due-to-breach-of-contract

[14] Bob Parsons, *35 million names registered in April. 32 million were part of a kiting scheme. A serious problem gets worse*, May 10, 2006, available at http://www.bobparsons.com/DomainKiting.html

Trade Commission, admitting that it had deceived customers into switching registrars when the customer was led to believe they were merely renewing their previous registrations.

Slamming continues, despite the FTC enforcement work. ICANN has a more immediate and direct way to restore integrity to domain name billing process, by rigorously enforcing its Registrar contracts, and de-certifying any Registrar who's caught slamming.

Expiration Extortion

"*Expiration Extortion*" describes a common practice of forcing a domain owner to pay an exorbitant fee to reinstate a name that's been allowed to expire. A leading registrar, for example, charges $80 to reinstate a domain name that costs only $8 to initially register. *Expiration Extortion* also describes the speculative game of snatching expiring domain names for resale to their former owner – or to the highest bidder.

Domain names are generally registered only for a year, although most owners renew before the year is up. Among all registrants, the average term for domain registration is 1.3 years.[15] Last year, the renewal rate for dot-com and dot-net domain names was 75%. That means 25% of names aren't renewed, so every day there's an average of 22,000 expiring domain names released by registries.

A company called Pool.com has perfected the science of snatching domain names as they expire, or "drop". Pool runs 80 servers in Sterling, Virginia that fire into action every day when dropped domain names are released at 2pm. According to Pool.com's president, Taryn Naidu, "*It's like going to the horse races every day*."[16] The race is won by whichever company, blasting multiple commands per second, snatches the dropped domain name.

Imagine if Pool.com were in the business of buying expired auto registrations instead of expiring domain names. Pool could snag your car registration if you failed to renew it by the expiration date, then sell the registration back to you or to another bidder who's willing to pay more.

Parking of Generic Terms

This fast-growing practice involves registering generic names, such as "consulting.com", which have little value in themselves but can generate revenue by carrying minimal content and advertising. Unsuspecting visitors to www.antidepressants.com might think they have found a site with reliable information regarding depression medications. But in fact, there is no content – only links to paid ads parked on the pseudo-site by a speculator looking to prey on people looking for helpful information.

Parking ads on otherwise unused sites like this is not only deceptive and confusing to the customer, it clutters the Internet the same way that unsightly billboards clutter the landscape along many of our nation's highways. This clutter undermines the value of the Internet for legitimate businesses and organizations, and misleads individuals searching for meaningful information.

ICANN's Agreements with Registries and Registrars can Promote DNS Integrity

Small businesses are increasingly frustrated and concerned about abusive domain name practices like squatting and slamming. Is ICANN doing enough to maintain the integrity of the DNS marketplace?

---

[15] ASCII Com/Net for Q1 2006

[16] As quoted by Peter Hum, "The New Cybersquatting: What'$ in a Name," The Ottawa Citizen, March 16, 2006.

Not a single one of the over five hundred registrars has been de-certified by ICANN, despite dodgy practices by some. Dotster, one of the largest registrars, was recently sued for allegedly participating in a massive typo-squatting campaign.[17] Dotster is accused of abusing its status as a registrar by sampling hundreds of domain names that closely resemble true names and then keeping only those that generated enough traffic to justify the registration fee.

Nevertheless, ICANN seems to grasp the seriousness of maintaining integrity of the DNS marketplace, judging by the new registry contract proposed for .com and subsequent TLD registries. In its new registry agreement for .com, ICANN indicates the potential for "prohibitions on warehousing of or speculation in domain names by registries or registrars."[18] An additional provision requires a registry operator to meet any future "consensus policy" adopted by ICANN to improve security and stability and to resolve disputes about domain names.

ICANN is managing DNS availability and integrity concerns contractually, through agreements with registries and registrars. However, a few large businesses have complained about ICANN's management of registry contracts, carrying their complaints here to Washington and requesting that the Commerce Department and this Committee reject ICANN's new agreement to run the .com registry. They complain that these registry contracts would create "perpetual monopolies" by granting exclusive contracts with presumption of renewal if the operator has met all performance requirements. ICANN's new contracts may not be perfect, but this criticism is misguided and self-serving.

First, an *exclusive* contract is essential to focus responsibility and accountability on the vendor running any single registry. The same is true for many outsourcing contracts that require accountability and consistency in the delivery of critical services, especially for infrastructure services that require significant investments.

Second, renewal options are common in longer-term service contracts to provide incentives for making investments that improve vendor performance. For example, the operators of the cafeteria downstairs might invest in a new grill or espresso machine if they're confident that their contract would be renewed upon expiration. And landlords often give tenants a purchase option as an incentive to maintain and improve the property.

Renewal options are already included in ICANN's existing registry contracts. Moreover, ICANN's new registry contracts require operators to implement any future policies adopted by ICANN to improve security and resolve domain name disputes. While such open-ended obligations could be difficult for any operator to meet, NetChoice would join those objecting to renewal if the incumbent registry operator failed to satisfy the contract's requirements.

An exclusive, renewable contract is therefore typical for infrastructure services that require single-vendor accountability and continuity. Moreover it provides incentives for investment, even during the final years of the contract. What, then, is the real nature of this complaint?

The largest registrars must approve fees that presently provide most of ICANN's funding. I attended the ICANN meeting in Vancouver last December, where the Finance Committee chair complained that ICANN expenditures were being delayed and possibly diminished because registrars had not yet approved the fees in the budget that was adopted for 2005-06.

---

[17] Declan McCullagh, *Registrar Named in Massive Cybersquatting Suit*, June 5, 2006, available at http://news.zdnet.co.uk/internet/0,39020369,39273075,00.htm

[18] Draft Registry Agreement, Section III.1(b), page 4, at http://www.icann.org/topics/vrsn-settlement/revised-com-agreement-clean-29jan06.pdf

ICANN's new registry contracts, however, would reduce the leverage held by large registrars today. When ICANN wants to make investments to ensure the Internet's security and stability, ICANN should not have to beg a "permission slip" from registrars—many of whom have little interest in security or stability.

From all appearances, this loss of leverage is why a few large registrars have pressed Congress and the Commerce Department to reject the new .com contract. ICANN can always improve its contracts, but complaints about a perpetual monopoly in the registry agreement are without merit.

The Committee should not let the loaded discussion of the registry contract distract it from acknowledging that ICANN's DNS management is working—even in the face of challenges to DNS availability and integrity. Furthermore, this Committee should consider the alternatives to ICANN management. ICANN's management duties are threatened by outside forces that could become serious in the near future if ICANN fails to do its job properly or if it becomes overburdened with governance duties beyond its managerial role. Two major threats are United Nations encroachment on ICANN and a potential splintering of the Internet.

The Threat of United Nations Encroachment on ICANN

There's a real and growing risk that ICANN's technical role for managing domain names will be encroached upon by the United Nations. The UN organized a World Summit on the Information Society last year to discuss Internet Governance. A UN working group then released a report that included controversial policy recommendations for the future of the Internet. Thanks largely to a unanimous resolution from Congress in November 2005, representatives from the international community allowed ICANN to continue managing the Internet under U.S. oversight, for the time being.

At the same time, the UN formed a new organization, the Internet Governance Forum, which meets for the first time in Athens next month. The current agenda for Athens includes workshops on a diverse range of societal issues, such as the "Greening of IT" through "legal and institutional mechanisms which strengthen the capacity of civil society for participation in decision-making."

While ICANN is far from a perfect manager, it provides the needed separation between Internet technical operations and governments. ICANN's bottom-up coordination of technical functions is the best way to preserve the democratic and decentralized character of the Internet. If there's anything that everyone at today's hearing should be able to agree upon, it's that we need ICANN to be strong and independent so it can fend-off interference from the UN and from governments.

DNS control by the UN or other governmental body would have significant economic and cultural effects. The decision making process would be even slower than it is now; the result would be a technological lag that could prevent the implementation of new technologies and processes that would benefit the DNS and its use in e-commerce.

Economic development and "social engineering" projects could interfere with essential technical management functions. Some nations, most notably China, maintain censorship controls on internet content available to their citizens. In a government-controlled ICANN, these nations might call for technical changes to facilitate censorship, tempting other regimes to restrict content access.

However, it would be a risky strategy for the US and ICANN to ignore the voices of the UN and other governments. That could lead to an unlikely, though highly undesirable outcome—splintering of the Internet.

A Splintered Internet Threatens All of Us – Not Just ICANN

In the brief history of the Internet, ICANN has not always been the only keeper of the domain name system. Alternative domain name systems still exist today, and are

trivial to create, as a technical matter. The consequences of a split internet, however, may not be trivial.

A split internet root would lead to a split in DNS policies, which could impair information security technologies, delivery of email, secure e-commerce transactions, trademark enforcement, and other forms of consumer protection. A split isn't likely, but ICANN and the U.S. Government need to be cognizant of the risk that a large nation or multi-national group could easily establish its own DNS.

How Can the U.S. Government and ICANN Make Internet Governance Work Better?

ICANN currently manages a DNS that generally works well for businesses and end users. However, the DNS is facing new attacks on availability and an erosion of integrity, calling for better contract management by ICANN and greater vigilance by consumer protection officials. ICANN must also withstand UN encroachment and avoid possible splintering of the Internet, challenges that could be met by ICANN and U.S. policymakers through these recommendations:

1. The U.S. Government should develop a "lighter touch" in its ICANN oversight.

The U.S. Government must avoid giving the international community any excuse to claim that the U.S. is being heavy-handed in Internet governance. From this point onward, U.S. actions should demonstrate a "lighter touch" in its ICANN oversight.

The U.S. Government is said to have unduly influenced ICANN's re-designation of registry operators for two country-code top-level domains (ccTLDs), and these instances have become legendary among critics of U.S. oversight. While there were valid reasons for the re-delegation of the Iraq and Australia ccTLDs, critics cite these instances to claim that the U.S. cannot be trusted with its oversight role.

The U.S. can take a major step to alleviate these concerns by unilaterally committing to a formal, internationalized process for changing a designated country top level domain. Countries regard their country code TLD as being under their sovereign authority, so they are entitled to designate their own registry. ICANN should respect those decisions, subject to security or stability qualifications and allowing for expedited re-designation during emergencies. The key is to balance the sovereignty of local communities while ensuring the unity, availability, and integrity of the DNS. A detailed process for this internationalization can be developed, such as one suggested by J. Beckwith Burr and Marilyn Cade.[19]

Another area where the U.S should show a lighter touch is in the launch of new top level domains. In 2005, the U.S. Government asked ICANN to delay the launch of the .xxx domain, designated for adult content. The proposal for .xxx had already made it through the ICANN approval processes, including opportunities for governments to comment. Although Brazil and France expressed similar reservations about .xxx, critics complain that U.S. abused its oversight role by overriding a DNS management decision that rightly belongs under ICANN purview.

2. The expiring Memorandum of Understanding should transition into a long-term agreement.

The current Memorandum of Understanding (MoU) between the U.S. and ICANN expires on September 30, 2006. Six previous expirations were marked by

[19] Burr, J. Beckwith and Cade, Marilyn S, in a letter submitted to NTIA regarding the Transition of the Technical Coordination and Management of the Internet DNS and Addressing System to the private sector, July 13, 2006, at http://www.ntia.doc.gov/ntiahome/domainname/dnstransition/comments/dnstrans_comment0643.pdf

amendments to extend the MoU and specify further milestones for ICANN to fully transition to private sector management.

Repeated extensions and milestones imply that the U.S. Government will one day cede all authority over ICANN and the "master copy" of the DNS root server. We believe the U.S. should formalize its long-term intention to keep the authoritative root distribution server physically located in the United States. This would send a clear signal that moving the root server is not an option. As with the back-stop agreements, this is necessary to ensure the availability and integrity of the DNS—no other purposes should be implied or intended.

3. The U.S. Government should maintain "back-stop" agreements for major registry operators and numbering authorities.

Presently, the U.S. Government has contingency agreements with operators of the authoritative root server, just as a back-stop in case ICANN were unable to execute its current responsibilities. It's prudent for the U.S. to continue this practice as a way to guarantee DNS availability to business and consumer interests both here and abroad.

4. ICANN and Governments should make the Government Advisory Committee (GAC) more involved and responsive.

Governments are not nearly as effective as they should be when participating in ICANN policy development. Government representatives often disregard target dates established in the policy development process by failing to provide timely and responsive comments at the time when policies are being formulated. What's more, some government comments have reflected more rhetoric than reality when characterizing the potential impact of proposed ICANN policies. Finally, ICANN decisions should not be held hostage when governments cannot reach consensus—government input should be given even where it does not represent a consensus position.

5. ICANN should improve the reach and transparency of stakeholder involvement.

Whenever ICANN supporting organizations and advisory committees present their official positions to the ICANN Board and community, they should reveal the degree of consensus achieved and the range of views. ICANN should encourage constituencies and advisory committees to report voting results, if any votes were taken. More important, ICANN's Board should request fuller disclosure of dissenting opinions and alternatives considered.

A recent example where this form of transparency worked well is the GNSO Council report on alternative formulations for the purpose of Whois. As this report showed, a bottom-up process can attempt to forge consensus, but should not suppress dissenting views. Moreover, ICANN outsiders would more readily participate when they see that dissenting views and alternatives are presented alongside majority views when constituencies pass advice along to ICANN's Board.

Conclusion

ICANN is a work-in-progress on the way to a bold and optimistic vision. I can think of no precedent for a multi-national, public-private partnership to manage an enterprise as complex and dynamic as the Internet.

The DNS has become an irresistible target for hackers, criminals, and unfair or deceptive practices, all of which endanger its availability and integrity. ICANN has made progress in its 7 year history, but it needs more operational experience to merit greater independence from U.S. Government oversight.

I close by thanking the Committee for holding this important hearing and I look forward to your questions.

MR. UPTON. Thank you. Mr. Lenard.

MR. LENARD. Thank you, Chairman Upton, members of the subcommittee. Thank you for this opportunity to express my views on the ongoing experiment in Internet governance that is ICANN.

The Internet is now the main driver of the digital economy, not only a global marketplace but also a means to communicate and contribute information more efficiently and more widely than ever before. How we govern the Internet has far-reaching economic, political and social ramifications. It can determine whether the Internet continues to flourish and grow or whether it gets bogged down by bureaucratic and politicized decision making.

My testimony makes three basic points. First, for all the controversy that has at various times surrounded the current government's arrangement, it is, as seems to be generally the view expressed here today, far superior to the alternative multilateral arrangements that have been proposed. There are many countries that do not share our commitment to promoting innovation, free markets and the free flow of information. And it is not difficult to envision a governing structure that would be far less friendly to the development of the Internet than the one we now have. Some other governments clearly are more prone to want to control the content that is available on the Internet. Governments may impede technical advances that now occur routinely in response to market forces in order to further their political and economic agendas. It is likely that a multilateral organization would adopt a more heavy-handed approach to Internet governance and that governance procedures would be used by countries to try to gain competitive advantages over each other.

Second point, having said all that, ICANN needs to resist its tendency toward becoming an economic regulatory agency and limit itself to administering the technical aspects of the domain names. In the current competitive environment in which customers are confused by the number of alternative and country code TLDs, there is no need for a regulatory approach with, for example, competitive bidding or price regulation to avoid the exercise of market power. We should give competing registry operators quasi property rights to their TLD registries in order to improve their incentives to invest in their business and maintain the quality of their TLD brands. These incentives are severely dampened if the registry operator knows that the rights to operate the registry can be lost when the contract expires. Giving incumbents the presumptive right of renewal is pro-competitive, and similarly, registries

should not face barriers if they want to offer new vertically related services.

Third, to ensure that the market for registry services is as competitive as possible, ICANN should free up entry and let the market determine the number of top level domains. ICANN's policies still limit competition in the TLD market as evidenced by the fact that ICANN has approved only a relatively small number of applications for new TLDs that it has received. The market should determine the number of TLDs available and ICANN should only disapprove applications if there are legitimate technical reasons for doing so. Innovation in the IT sector, in which the Internet obviously plays a key role, has been the engine of growth in the U.S., the basis for an economic performance over the past decade that sets us apart from much of the rest of the world. Maintaining a climate of innovation benefits every one, not just the U.S. However, the U.S. has perhaps more to lose if the pace of innovation slows because of more bureaucratic process and a more heavy-handed regulatory approach.

Despite ICANN's defects, the Internet has flourished under the current Internet governance arrangement, and I would not have the same confidence with respect to a multilateral arrangement. But ICANN can be even more light handed and pro-competitive, and that should be its goal. Thank you very much.

[The prepared statement of Thomas Lenard follows:]

PREPARED STATEMENT OF THOMAS M. LENARD, SENIOR VICE PRESIDENT FOR RESEARCH, THE PROGRESS & FREEDOM FOUNDATION

Chairman Upton, Chairman Stearns, Ranking Members Markey and Schakowsky, and members of the Committee. Thank you for this opportunity to express my views on the ongoing experiment in Internet governance that is ICANN and how well it is working. My name is Thomas Lenard and I am a senior fellow and senior vice president for research at The Progress & Freedom Foundation. PFF is a non-partisan, non-profit think tank that focuses on public policy issues that affect the digital revolution and the information economy generally.

The Internet is now the main driver of the digital economy—not only a global marketplace, but also a means to communicate and distribute information more efficiently and more widely than ever before. How we govern the Internet has far-reaching economic, political and social ramifications. It can determine whether the Internet continues to flourish and grow, or whether it gets bogged down by bureaucratic and politicized decision making.

My views on ICANN's performance, briefly, are as follows:

- ICANN has made progress and is continuing to improve. Despite some problems that have plagued the organization, the Internet has flourished during the period that ICANN has been "in charge". This is due to ICANN's charter to concentrate its oversight on technical aspects of the domain name system (DNS) and its relatively light-handed approach.

- Moving ICANN's governance functions to a multilateral organization would be extremely risky. A multilateral organization is likely to be far more intrusive and regulatory, which would put the future development of the Internet at risk.
- However, ICANN must resist the drift toward becoming an economic regulatory agency. There is already sufficient competition in the markets for domain names to move away from ICANN's regulatory approach.
- To ensure that the market for registry services is as competitive as possible, ICANN should free up entry and let the market determine the number of TLDs (top-level domains).

Multilateral Governance

There are a number of countries that believe that Internet governance should be shifted to a multilateral organization of some sort. The Congress expressed its disagreement with that view in a resolution passed last year. The agreement reached at the World Summit on the Information Society in Tunis in November 2005 assures that the current structure of Internet governance will remain in place, at least for the time being.

We should thank our very able diplomats for achieving the Tunis commitment, which is very important. For all the controversy that at various times has surrounded the current governance arrangement, and notwithstanding some criticisms I will discuss, it is far superior to the alternative multilateral arrangements that have been proposed. There are many countries that do not share our commitment to promoting innovation, free markets and the free flow of information. It is therefore not difficult to envision a governance structure that would be far less friendly to the development of the Internet than the one we now have. Some other governments clearly are more prone to want to control the content that is available on the Internet and limit the free flow of information. Governments may impede technical advances—advances that now occur in response to market forces—in order to further their political and economic agendas. It is likely that a multilateral organization would adopt a more heavy-handed approach to Internet governance and that governance processes would be used by countries to try to gain competitive advantages over each other.

Innovation in the IT sector—in which the Internet has played a key role—has been the engine of growth in the U.S., the basis for an economic performance over the past decade that sets us apart from much of the rest of the world. Maintaining a climate of innovation benefits everyone, not just the U.S. However, the U.S. has perhaps more to lose if the pace of innovation slows because of more bureaucratic processes and a more heavy-handed regulatory approach, which would be predictable if Internet governance were shifted to a multilateral organization.

Internet Governance and the Domain Name System

ICANN administers the DNS, which is essential for the operation of the Internet. Operationally, the DNS is organized as a hierarchy with top-level domains (TLDs), such as .com or .edu at the top. These TLDs are operated by registry operators who take requests for second-level domains—e.g., amazon.com—and determine whether they are available and, if so, register them. The registry operators maintain the database of all registered names so they can determine if domain names are available if requested. For the domain name system to work for Internet users, each domain name must resolve to a unique IP address, and the registries obviously are an essential part of that system.

All this suggests that the administration of the DNS is essentially a technical exercise, and ICANN, or any alternative system, is best if it limits itself to administering the technical aspects of the DNS. This view is reflected in the Department of Commerce's 1998 White Paper on DNS coordination and management, which set forth the following responsibilities for a DNS administrator:

1. To set policy for and direct the allocation of IP number blocks;
2. To oversee the operation of the Internet root server system;
3. To oversee policy for determining the circumstances under which new top level domains would be added to the root system; and
4. To coordinate the assignment of other Internet technical parameters as needed to maintain universal connectivity of the Internet.[1]

These are largely technical functions, with the exception of the third, which has a potentially significant economic policy element.

Competition and Regulation

From an economic standpoint, there are good efficiency reasons to have a single registry operator for each TLD. Because of this, it is sometimes assumed that registries should be viewed as monopolists and regulated accordingly. Indeed, this has been ICANN's approach:

- ICANN enters into agreements with registry operators, sometimes through a competitive bidding process, to operate a given registry under specific operational and service parameters. These parameters may include price ceilings (e.g., for the .com operator).
- At the end of the contract period, the right of the incumbent to renew the contract and continue to operate the registry is uncertain, even if its performance has been entirely satisfactory.
- The introduction of new services related to the core registry functions has been proscribed under the theory that such new businesses can be used to circumvent the established price ceilings.

The rationale for such regulation in an environment in which there is competition, even if not perfect competition, is very weak. A regulatory regime of the type that ICANN has been operating, including regulation of price and service quality, is at best a flawed tool, even for true monopolies. Notwithstanding the fact that there is only one registry operator for each TLD, there is a significant amount of competition between TLDs—from new gTLDs (generic TLDs, such as .info) and from the proliferation of ccTLDs (country code TLDs, such as .us). Indeed the ICANN board in a majority statement issued earlier this year indicated its view that the market for registry services was increasingly competitive:

> However, we firmly believe that ICANN is not equipped to be a price regulator, and we also believe that the rationale for such provisions in registry agreements is much weaker now than it was at the time the VeriSign agreement was originally made in 1998. At that time, VeriSign was the only gTLD registry operator, and .COM was, as a practical matter, the only commercially focused gTLD. Today, there are a number of gTLD alternatives to .COM, and several ccTLDs that have become much stronger alternatives than they were in years past. In addition, the incredibly competitive registrar market means that the opportunities for new gTLDs, both in existence and undoubtedly to come in the future, are greater than they have ever been. It may well be that .COM offers to at least some domain name registrants some value that other registries cannot offer, and thus the competitive price for a .COM registration may well be higher than for some alternatives. But price is only one metric in a competitive marketplace, and relative prices will affect consumer

[1] U.S. Department of Commerce, Statement of Policy on the Management of Internet Names and Addresses (Docket Number 980212036-8146-02) (available at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm).

> choices at the margin, so over time, we expect the registry market to become increasingly competitive. One way to hasten that evolution is to loosen the artificial constraints that have existed on the pricing of .COM and other registries. We began this process with the .NET agreement, and we now continue it with the .COM agreement, and we expect to continue along this path as we renegotiate agreements with other registries.[2]

In the current competitive environment, in which customers can choose between a number of alternative gTLDs and ccTLDs, there is no need for competitive bidding or price regulation to avoid the exercise of monopoly power and, in fact, such regulation is harmful. We should give competing registry operators quasi property rights to the TLD registry in order to improve their incentives to invest in their businesses and maintain the quality of their TLD "brand". These incentives are severely dampened if the registry operator knows that the rights to operate the registry can easily be lost when the contract expires. This implies that giving incumbents the presumptive right of renewal—e.g., the proposal to extend VeriSign's contract to operate the .com registry—is procompetitive. Similarly, registries should not face barriers if they want to offer vertically related services, which will enhance economic efficiency.

Having said all this, ICANN's policies still unduly limit competition in the TLD market. ICANN has approved only a relatively small number of the applications for new TLDs it has received. There is no good rationale for such a restrictive policy. The market should determine the number of TLDs available and ICANN should only disapprove applications if there are legitimate technical reasons for doing so.

Conclusion

The current Internet governance arrangement should not be set in stone, because we are dealing with a fast-changing technological environment. At this stage, however, there does not seem to be a good reason to make any significant change. Despite ICANN's defects, the Internet has flourished under the current Internet governance arrangement. I would not have that same confidence with respect to a multilateral governance arrangement. But, ICANN can be even more light-handed and pro-competitive in its approach to overseeing the DNS and that should be its goal.

MR. UPTON. Thank you.

Mr. Feld.

MR. FELD. Thank you. The question is not should we turn ICANN over to the U.N., nobody here thinks that, it would be disastrous. The number of ridiculous decisions that would be voted 147 to 3 within the first 2 weeks is staggering.

The real question is, one, why, despite that, were there so many people so upset with U.S. involvement with ICANN and with the way ICANN is running itself that this was even something that a lot of people

---

[2] Joint Statement from Affirmative Voting Board Members (available at http://www.icann.org/topics/vrsn-settlement/board-statements-section1.html).

were seriously talking about leading up to the World Summit on the Information Society.

This should never have gotten past suggestions batted around by a few folks in Geneva and some governments that are perpetually opposed to our interests. But even the European Union started to say, hmm, maybe it wouldn't be a bad idea. When there is that much unhappiness, we need to look at why.

The other problem is how do we get ICANN out of Internet governance. ICANN sadly has become what nobody wanted it to be, a really bad copy of the FCC making every mistake that the FCC has made on Internet time. We cycled through beauty contests for assignments of licenses, we are into the license renewal phase. I am looking forward to when we finally get the competitive options for TLDs.

And it is astounding how we are doing the same thing over and over again. This shows up in the question of what does stability mean. The AM/FM radio and television standards have been very stable, we are still using 1950s technology. We were hoping that that was not the kind of stability that we were going to see in the Internet, but the problem is, when you have control over the generic top level domain contracts, then you have huge debates of what do we mean by stability. The incident with Site Finder, where VeriSign unilaterally introduced a new service, is a classic example of a problem of mixed engineering, policy, and economics. Did it make it very inconvenient for a number of ISPs who were relying on dot coms to work the same way forever? Yes, a lot of people spent a lot of time up late at night, when it went online unexpectedly. But nobody has figured out a good process for how dot com is going to innovate, so that we are not 50 years from now working with the same kind of registry/registrar services.

We are also seeing real problems with the level of oversight that is being exercised by NTIA and by ICANN. On the one hand, everybody says they don't want to regulate, and NTIA says we are not the court of last resort, but the contract between VeriSign and ICANN is pending in front of NTIA in a way it stands before no other government. And, of course, when there is a possibility that somebody else might fix your problems, you attract people who are interested in having their problems fixed.

So what should we be doing? Because nobody wanted this 10 years ago. And it was around 10 years ago when we first started talking about this, and nobody supposedly wants it today. I think Mr. Twomey has been doing an excellent job, but I looked at the ICANN strategic plan, it is now up to $30 million, and people are talking about making enforcement mechanisms to it? You all know on this committee how much the FCC spends on an annual basis for enforcement, and that is one

country's issues. Are we prepared for ICANN's budget to go from $30 million, which it is now, to $250 million?

We need to do a number of things, as I have suggested in my testimony. One, in making the world more comfortable, we need to first find an appropriate forum to talk about the issues that a lot of the people in the world want to talk about in Internet governance. Happily, there now is one, the Internet Governance Forum, which will be starting in Athens. We should go and participate there and quietly slip ICANN and the DNS out the back door at the first opportunity because it doesn't belong in the Internet Governance debate. We need to resolve the relationship between ICANN and NTIA and be open and up front about it. If NTIA is going to be ICANN's permanent oversight, we need to say it. If there is a way that NTIA is going to let go, then we need to figure out how we are going to let go. But we can't keep having a discussion about NTIA letting go when we don't really mean it. That gets people in the world very annoyed at us because nobody in the world likes a tease.

Finally, there is ICANN. There is a real problem with accountability and representation. The vast majority of people who have ever actually dealt with ICANN from the bottom up agree with that. I understand Dr. Twomey's remark that nobody has used the accountability mechanism that is right now at ICANN. There are two possible reasons for that, either because everybody is so happy and wonderful--which, given the public comments, is not the case--or because nobody thinks that that process is worth bothering with.

So I would urge NTIA, as it reviews the contract, to force ICANN to re-examine its accountability mechanisms. Thank you.

MR. UPTON. Thank you.

[The prepared statement of Harold Feld follows:]

PREPARED STATEMENT OF HAROLD FELD, SENIOR VICE PRESIDENT, MEDIA ACCESS PROJECT

Executive Summary of Prepared Testimony of Harold Feld
Senior Vice President, Media Access Project

The question is not "should we turn ICANN over to the U.N., as some have phrased it. We should not. Nor is the relevant question "does ICANN do internet governance well?" It doesn't, because it shouldn't be doing it in the first place. Unfortunately, ICANN has morphed into what nobody wanted, the Federal Communications Commission (FCC) of the internet. Worse, it does it badly, repeating every mistake ever made by the FCC in its 70+ years of history – on internet time.

The real questions, in my opinion at least, are "how to get ICANN out of the internet governance debate" and "how to make sure ICANN does the job it has to do better." Answering the first question is significantly easier than the second. For the reasons explained below, I recommend the following:

To Get ICANN Out of the Internet Governance Debate:

- The U.S. should embrace the Internet Governance Forum (the successor to the World Summit on the Information Society) as the proper place to talk about "internet governance," a category that excludes the technical management of the domain name system but includes the much more interesting things -- like cybercrime, censorship, and security -- most governments really want to talk about. Hopefully, we can remove ICANN as an attractive target for topics it has no business or interest in addressing.
- NTIA should not be the "court of last resort" for ICANN decisions, a *de facto* role it unwillingly occupies now because it can veto any important ICANN decision.
- The USG should appoint someone other than NTIA to represent the U.S. in the GAC (or transfer the MoU to a different agency. Expecting the world to treat the NTIA representative in the GAC as just another government representative when the same person has veto power over ICANN decisions is simply unreasonable.
- NTIA needs to either say up front that it will never fully transfer authority over the DNS to ICANN or it needs to set a clear path (with a projected time line) for the transfer to take place. Real dialog with concerned governments and other stakeholders cannot be premised on false positions or ambiguity on this vital issue. If full transfer is off the table, say so and begin discussions on how to make other governments as comfortable as possible with that reality.

To Get ICANN Functioning More Efficiently:

- NTIA cannot act unilaterally on ICANN's internal structures, but can use the MoU renewal and threat of rebid to force critical changes.
- First and foremost, ICANN must have a meaningful accountability mechanism. If ICANN is the FCC of the internet, it needs a D.C. Circuit Court of Appeals to keep it from exceeding its mandate and to protect DNS users (meaning everyone) from arbitrary and capricious decision making.
- ICANN needs some kind of mechanism to provide all stakeholders a way of participating. Right now, there is no formal way in which any person or entity can participate in ICANN and hope to influence ICANN's process for developing policy if he or she does not fit into one of ICANN's six arbitrary "constituencies." Worse, these Constituencies were created based on which interests were present in 1998/1999 and had enough clout to force representation. The world has changed a lot since then, particularly with regard to who uses the internet. ICANN's processes need to reflect these changes.
- ICANN needs to stop pretending it doesn't do regulation and learn to separate regulatory issues like competition policy from technical coordination. If ICANN is going to set tariffs and price caps, which is essentially what it does for domain names, it needs to stop navigating by the seat of its pants and figure out how to come up with real numbers that makes sense.

I wish I had more specific solutions for ICANN's problems. But NTIA has gotten good recommendations from a number of interested parties. I recommend starting with the comments of the Internet Governance Project (IGP), a consortium of academics interested in ICANN and internet governance. They have a lot of relevant knowledge and experience.

Which, I suppose, leads to one last recommendation. It is high time for ICANN and NTIA to stop circling the wagons against critics and start looking outsider its insider circle for advice. The days in which only engineers had useful things to say about DNS

management, for better or for worse, are over. Public policy, economics, and law are as much specialties as engineering. Yet ICANN's Board and many key supporters continue to insist that only engineering expertise matters because ICANN is only about technical coordination. Until ICANN recognizes that it does real regulation rather than just technical coordination, it will lack the expertise it needs to do its job properly.

Good afternoon. My name is Harold Feld. I am Senior Vice President of the Media Access Project (MAP), a 35-year old non-profit public interest law firm protecting the public's First Amendment right to speak and hear information from a diversity of sources in the electronic media. MAP is a member in good standing of ICANN's non-commercial user constituency (NCUC).

The question is not "should we turn ICANN over to the U.N., as some have phrased it. We should not. Nor is the relevant question "does ICANN do internet governance well?" It doesn't, because it shouldn't be doing it in the first place. Unfortunately, ICANN has morphed into what nobody wanted, the Federal Communications Commission (FCC) of the internet. Worse, it does it badly, repeating every mistake ever made by the FCC in its 70+ years of history – on internet time.

The real questions, in my opinion at least, are "how to get ICANN out of the internet governance debate" and "how to make sure ICANN does the job it has to do better." Answering the first question is significantly easier than the second. For the reasons explained below, I recommend the following:

To Get ICANN Out of the Internet Governance Debate:

- The U.S. should embrace the Internet Governance Forum (the successor to the World Summit on the Information Society) as the proper place to talk about "internet governance," a category that excludes the technical management of the domain name system but includes the much more interesting things -- like cybercrime, censorship, and security -- most governments really want to talk about. Hopefully, we can remove ICANN as an attractive target for topics it has no business or interest in addressing.
- NTIA should not be the "court of last resort" for ICANN decisions, a *de facto* role it unwillingly occupies now because it can veto any important ICANN decision.
- The USG should appoint someone other than NTIA to represent the U.S. in the GAC (or transfer the MoU to a different agency. Expecting the world to treat the NTIA representative in the GAC as just another government representative when the same person has veto power over ICANN decisions is simply unreasonable.
- NTIA needs to either say up front that it will never fully transfer authority over the DNS to ICANN or it needs to set a clear path (with a projected time line) for the transfer to take place. Real dialog with concerned governments and other stakeholders cannot be premised on false positions or ambiguity on this vital issue. If full transfer is off the table, say so and begin discussions on how to make other governments as comfortable as possible with that reality.

To Get ICANN Functioning More Efficiently:

- NTIA cannot act unilaterally on ICANN's internal structures, but can use the MoU renewal and threat of rebid to force critical changes.
- First and foremost, ICANN must have a meaningful accountability mechanism. If ICANN is the FCC of the internet, it needs a D.C. Circuit Court of Appeals to keep it from exceeding its mandate and to protect DNS users (meaning everyone) from arbitrary and capricious decision making.

- ICANN needs some kind of mechanism to provide all stakeholders a way of participating. Right now, there is no formal way in which any person or entity can participate in ICANN and hope to influence ICANN's process for developing policy if he or she does not fit into one of ICANN's six arbitrary "constituencies." Worse, these Constituencies were created based on which interests were present in 1998/1999 and had enough clout to force representation. The world has changed a lot since then, particularly with regard to who uses the internet. ICANN's processes need to reflect these changes.
- ICANN needs to stop pretending it doesn't do regulation and learn to separate regulatory issues like competition policy from technical coordination. If ICANN is going to set tariffs and price caps, which is essentially what it does for domain names, it needs to stop navigating by the seat of its pants and figure out how to come up with real numbers that makes sense.

I wish I had more specific solutions for ICANN's problems. But NTIA has gotten good recommendations from a number of interested parties. I recommend starting with the comments of the Internet Governance Project (IGP), a consortium of academics interested in ICANN and internet governance. They have a lot of relevant knowledge and experience.

Which, I suppose, leads to one last recommendation. It is high time for ICANN and NTIA to stop circling the wagons against critics and start looking outsider its insider circle for advice. The days in which only engineers had useful things to say about DNS management, for better or for worse, are over. Public policy, economics, and law are as much specialties as engineering. Yet ICANN's Board and many key supporters continue to insist that only engineering expertise matters because ICANN is only about technical coordination. Until ICANN recognizes that it does real regulation rather than just technical coordination, it will lack the expertise it needs to do its job properly.

Background

Since 1997, I have participated in the debate over ICANN and the broader "internet governance" concepts that ICANN has alternately sought to embrace or avoid. In that time, I served as an NCUC representative to the Names Council (now the Generic Names Support Organization), served as NCUC's representative on the advisory board of the Public Interest Registry (the registry for the .org generic top level domain), participated in various ICANN processes, task forces, and meetings. Recently, however, I have been primarily as an observer rather than a participant. It is therefore from the perspective of an observer that I offer my testimony today.

In 2003, I wrote that ICANN was fundamentally flawed because it arose from a compromise among competing interests and could not possibly hope to satisfy them all.[1] The traditional internet community, members of which continued to control important pieces of the internet's infrastructure, wanted a narrowly focused organization that could act as a "heat shield" against intrusive political actors or business interests. Trade associations concerned with "cybersquatting" and other issues involving intellectual property wanted a convenient way to address their concerns. Businesses and governments wanted stability and a place to raise issues related to the name system. This activity attracted the interest of civil society advocates, such as myself, who were concerned that the central critical resource of the internet would fall under the unaccountable control of one or more interests indifferent to the impact of decisions on DNS on free expression, privacy and consumer protection.

---

[1]Harold Feld, "Structured to fail: ICANN and the 'Privatization' Experiment," in *Who Rules the Net?* CATO (2003).

The resulting compromise structure that became ICANN survives by the happy chance that its dysfunctionalities have so far cancelled each other out. On the one hand, ICANN decisions are made by a Board of Directors accountable to no political authority and with no meaningful appeal of its decisions. On the other had, the process by which ICANN distills "consensus" is so cumbersome, complicated, frustrating and difficult to manage that little actually gets done. In some ways, this resembles the complicated system for passing laws envisioned in the Constitution, where our libertarian forbears compromised between Federalists like Hamilton and anti-Federalists who feared a strong central government. But frustration with this system does occasionally build to a point where the continued existence of ICANN is actually threatened.

Frustration with ICANN has precipitated political crisis twice in ICANN's relatively brief history. The first time, in 2002, the ICANN Board pushed too hard and too fast to assert control over critical aspects of the Internet naming structure. Notable missteps included:

- Endless contract negotiations between staff for new registry and registrar services that embodied the worst in unaccountable bureaucratic rulemakings;
- Extension of director terms and elimination of promised accountability mechanisms such as electing Directors;
- Threatening to withhold needed services to country code top level domain (ccTLD) root zone files unless the ccTLDs entered into binding contracts with ICANN;
- Simultaneously seeking to embrace governments by redelegating the .AU ccTLD at the request of the Australian government while formally limiting the role of governments to the Government Advisory Committee (GAC); and,
- Simultaneously embracing the dominant registry Verisign by modifying the agreement under which Verisign operated the ".com" domain while allowing industry rivals to leverage ICANN's processes to impose onerous regulatory hurdles before Verisign could bring new services to market.

Throw in accusations of cronyism, a ballooning budget paid for by fees ICANN imposed on entities ICANN regulated, and increasing concern by foreign governments that the U.S. government and U.S. businesses were exercising too much control over the internet's naming structure, and it is no surprise that the Department of Commerce faced serious pressure in 2002 to find another contractor to handle ICANN's duties or otherwise force ICANN to change how it conducted business.

ICANN survived the 2002 crisis for several reasons. First and foremost, no one could come up with a better solution for how to manage the internet naming system that commanded anything close to consensus. Second, ICANN actively undertook steps to placate its most powerful critics. Several of the more controversial directors allowed their terms to end, bringing in much needed fresh blood an new perspectives. The hiring of Dr. Paul Twomey, an Australian with experience in government, non-governmental organizations and the private sector, as President likewise helped diffuse hostility from foreign governments and disgruntled stakeholders. ICANN provided a more formal role for the GAC, clarified to some degree its policy formation structure, and agreed to move forward (in a limited way) on some of the more pressing issues surrounding the DNS.

Nevertheless, problems continued. Notable flash points included the controversy over Verisign's unilateral decision to introduce a new service, "Site Finder,"in September 2003. Prior to the introduction of Site Finder, entering a non-existent URL ending in .com or .net returned a message that the requested domain did not exist (although numerous browser plug-ins would take the opportunity to redirect users to sites where they could register the non-existent name). When Verisign introduced Site Finder, entering a non-existing URL would direct the user to the Site Finder website. In response to widespread complaints that this new service at the registry level created potential

instabilities, ICANN directed Verisign to withdraw Site Finder. Verisign replied that it would voluntarily withdraw the service, but maintained that ICANN had no authority to regulate its service offerings. Verisign also complained that to the extent it had failed to follow ICANN processes, this was because it was impossible to determine what the correct processes were.

The incident highlighted one of the chief problems for ICANN. On the one hand, an unannounced unilateral change at the registry level, particularly of the dominant generic top level domains, could potentially create serious issues for ISPs and others relying on the stability of the registry service. On the other hand, ICANN was not supposed to act as a regulatory body. Its supporters had argued time and again that requiring businesses to seek regulatory approval for new services would prove the death knell of innovation on the internet. And, if ICANN could regulate Verisign's services, what were the limits of that authority? Was there any appeal for Verisign, or Verisign's competitors, once the ICANN Board made a decision?

Another issue that caused world governments to take notice was the redelegation of Iraq's country code, the .iq ccTLD. According to the official report by the Internet Assigned Numbers Authority (IANA)[2], the .iq ccTLD was never activated. In 2002, the original recipient of the .iq delegation was arrested for laundering money for Hamas. In 2004, the Coalition Provisional Government requested redelegation of .iq. In 2005, the IANA redelegated the .iq ccTLD to the National Communications and Media Commission of Iraq.

In many ways, this decision was entirely unremarkable; ICANN has redelegated ccTLDs before. But the fact that this took place in secret (as other redelegation decisions had) in the context of deep international suspicion about the United States involvement in Iraq and U.S. control over the DNS aroused concerns that the U.S. had simply ordered its contractor ICANN to make a unilateral change to the .iq ccTLD. As many countries increasingly regard their ccTLD as both an aspect of their sovereignty and as critical to their commerce and information infrastructure, the fear that the U.S. exercised too much control over the DNS gained significant currency in the international community.

These fears were further stoked by the controversy surrounding inclusion of the proposed .XXX gTLD. In the summer of 2005, ICANN staff completed negotiations with the proposed .XXX registry and the Board of Directors scheduled a vote. This triggered protests from a number of governments through their representatives in the GAC. In addition, however, a significant number of opponents to the .XXX gTLD appealed directly to NTIA to "veto" any ICANN decision to include the .XXX gTLD in the root.

This put NTIA in a profoundly awkward position. As representative of the U.S. government to the GAC, it is entirely appropriate for the Administrator of NTIA (or delegated representative) to express opinions consistent with U.S. interests. Indeed, it would seriously disadvantage the U.S. if NTIA could ***not*** participate fully in the GAC. At the same time, no one can forget that the Administrator of NTIA is the only government representative in the world with the ability to veto a decision by the ICANN Board of Directors. This inevitably makes NTIA a target for lobbying by parties with interests before ICANN, and opens NTIA to accusations of "regulating by raised eyebrow" when it forcefully advocates for particular positions.

Meanwhile, between 2003 and 2005, ICANN continued to stumble along. While improved somewhat after the reforms of 2002-03, ICANN's consensus and policy development processes still move incredibly slowly and inefficiently, with no clear understanding of the Board ultimately determines the "consensus" and no means of

---

[2]http://www.iana.org/reports/iq-report-05aug05.pdf. Among the many complicating factors in DNS management is the continued persistence of the IANA as a quasi-entity and quasi-function within the ICANN structure.

appealing ICANN decisions. This lack of accountability, combined with an ever increasing bureaucracy and budget (ICANN now employs over 50 staff members and has a budget of $30 Million – not bad for a small organization dedicated to technical coordination), has bred considerable frustration among participants in the ICANN process. It is telling to me that, although I stopped significant participation in ICANN in 2003, I could attend the meeting scheduled for December 2-8 in Sao Paulo and find familiar topics such as the implementation of internationalized domain names, the purpose of the WHOIS registry, and policy for including new gTLDs on a regular basis still under discussion.

Worse, because ICANN's mandate remains ill-defined, it continues to attract the attention of interested parties and world governments interested in "Internet governance," the very thing ICANN's founders intended to avoid. ICANN has no mandate or expertise for how to bring the benefits of the internet to developing nations. Nor should it serve as a global police officer for internet content. There are many issues of worth considered under the rubric of "internet governance," but ICANN is precisely the wrong place to settle them. On the other hand, if trade organizations can successfully ask ICANN to solve their intellectual property enforcement issues, why shouldn't other interest groups or governments look to ICANN to solve what they consider to be the pressing issues of the day?

In November of 2005, the frustration with ICANN again boiled over, this time at the World Summit on the Information Society (WSIS). As part of the preparation for WSIS, a Working Group on Internet Governance (WGIG) examined both governance of the naming system and other issues loosely related as "internet governance." Although WGIG itself was only intended as one part of a broader WSIS agenda, the primary focus of the WSIS meeting in Tunis turned to the efforts of various governments to move ICANN out of U.S. control and the efforts of other participants to use the dissatisfaction around ICANN to create real change in its operation.[3] This, in turn, prompted the House of Representatives to approve overwhelmingly a resolution supporting continued management of the DNS by ICANN under the authority of NTIA.

After considerable negotiation at the WSIS meeting in Tunis, world governments agreed to accept the basic arrangements under which ICANN manages the DNS. In exchange, the United States agreed to participate in a new international "Internet Governance Forum" (IGF). The IGF was explicitly designed to include the wide range of issues relating to "internet governance" that fall outside the proper role of ICANN. The IGF will continue discussion on a wide variety of issues for five years. The first formal meeting of the IGF will take place in Athens, Greece on October 30, 2006.

On September 30, 2006, the existing Memorandum of Understanding (MoU) between ICANN and the Department of Commerce will expire. It is a forgone conclusion that NTIA will renew the MoU. The critical questions are under what terms, and with what expectations.

DISCUSSION

In considering what level of oversight NTIA should exercise over ICANN through the MoU, and what level of oversight Congress should exercise over NTIA, it is important to distinguish between separate issues that are frequently confused. In recent debates the question is usually phrased as whether some sort of international intergovernmental organization, such as the U.N., should assume control of ICANN.

---

[3]A number of useful background pieces on WSIS, WGIG, and ICANN Reform can be found at the Internet Governance Project, http://www.igp.org. The IGP is a consortium of academics from a variety of disciplines relevant to the questions of internet governance. For a good, narrative background piece on WSIS and the WGIG *see* Andrew Updegrove, "WSIS, ICANN and the Future of the Internet," available at http://www.consortiuminfo.org/bulletins/nov05.php#feature

This question is easily answered "no," at least by anyone concerned with preserving freedom of expression on the Internet.

But the easy answer to this question hides matters deserving of significant attention. It is often used as a distraction from examining the very real problems that still afflict ICANN and its processes. ICANN can attribute its survival to date more to the lack of any real alternative capable of commanding consensus than to deep satisfaction with the status quo. Or, in an oft repeated observation by Representative Markey (D-MA), paraphrasing Winston Churchill, "ICANN is the worst form of Internet governance ever conceived, except for all the other forms proposed."

To dismiss international opposition to U.S. management of ICANN and concern about ICANN itself to the machinations of a few governments perpetually hostile to U.S. interests merely invites us to undertake the same cycle of argument again and again until something changes dramatically. When even usual allies of the United States at ICANN such as the European Union express concerns with continued U.S. management of ICANN, we should recognize a serious problem. We ignore the warning signals sent up at WSIS at our peril.

On the other hand, it is logical to ask why it matters whether governments are or are not satisfied with U.S. arrangement for management of the DNS. After all, at the end of the day, governments cannot force the U.S. to turn over its contracts or critical infrastructure if the U.S. declines to do so.

Two factors, however, mitigate against a such a unilateral approach. First, the debate over ICANN and internet governance takes part in a larger context of multilateral negotiations of importance to the United States. To respond to world governments with a simple "sucks to be you" is to invite retaliation – both subtle and gross – against U.S. companies and U.S. interests in other fora.

Second, a real danger exists in the form of "splitting the root." At it's heart, the DNS is simply a table that keeps a list of name servers that match domain names with internet protocol (IP) addresses used by machines to send internet traffic. Nothing prevents a country from creating its own master list and requiring by law that all ISPs within its boarders use this "alternate root" rather than the existing root. The problem arises if the "alternate root" has different information from the "authoritative root." If this happens, Internet traffic intended for the same recipient could go to different recipients. Predictions for the outcome of such an experiment range from ultimately beneficial (a minority view) to catastrophic (somewhat more broadly held view) to a range in between. At the very least, the existing global nature of the internet would be altered in ways that would impose significant costs on U.S. businesses and on people everywhere trying to communicate with one another.

"Splitting the root" is highly unlikely, in no small part because doing so imposes significant costs on the country isolating itself from the broader internet. But, like the existence of nuclear weapons, the possibility of splitting the root provides an incentive for the United States to continue to engage other countries.

Finally, leaving international considerations aside, the temptation to give ICANN a "free pass" because no one can find a better alternative that commands sufficient support imposes very real consequences on DNS management and on the people and businesses that rely on the DNS (which, at this point, is just about everyone). An ICANN incapable of commanding legitimacy cannot create consensus or coordinate needed improvements in the DNS as intended. An ICANN that remains unaccountable is a recipe for autocratic and ill-informed decision making, cronyism, and bureaucratic waste. ICANN's decisions can impact the civil liberties of millions of American citizens registering domain names in their personal capacities, and impose billions in hidden costs (both directly and through missed opportunities) on U.S. businesses.

At the same time, Congress and NTIA must approach reform of ICANN with considerable delicacy. Unilateral decisions to address concerns, however worthy, give

credence to the charge that the U.S. has a privileged position in internet domain name management that others resent.

I present therefore only some very surface recommendations. The first center on specific changes Congress and NTIA can make outside of ICANN to defuse the legitimate concerns raised by other governments. The second set of recommendations address ICANN specific problems that NTIA should attempt to remedy via the MoU renewal process.

Mitigating World Hostility

Embrace the Internet Governance Forum. It is understandable that, after WSIS, interested parties might resist the IGF as a continuation of the process by which hostile interests try to seize control of ICANN. But the IGF presents a tremendous opportunity to get ICANN out of the issue of "internet governance" by providing a proper forum to address issues of global concern. Too many people look to ICANN to resolve their "internet governance" problems – whether this means online gambling, digital inclusion, of "irresponsible" websites critical of totalitarian regimes – because there is no other forum in which to discuss these issues. Furthermore, because control of the DNS, the central bottleneck of the internet, offers a convenient means by which governments can hope to control content or levy fees similar to the manner which they have traditionally controlled and levied fees on broadcasting and telephony, it naturally attracts the attention of governments and others looking for global solutions to their perceived problem. While this last will continue to remain true for the foreseeable future, we can at least take steps to minimize the attractiveness of ICANN as a forum for "governance" issues by providing alternate fora for discussion.

U.S. participation in the IGF, particularly after the endorsement of ICANN by the WSIS participants, thus becomes the means by which the U.S. engages with other countries on critical internet issues as part of a multilateral process familiar to most governments and open to both civil society and private sector interests. By establishing IGF as the appropriate forum for these broad-ranging discussions, interest in leveraging ICANN as a forum for these discussions will diminish over time. While this will not satisfy those intent on attacking U.S. "dominance" of the DNS, it will help satisfy countries and interests whose chief frustration is the lack of a suitable forum to resolve pressing internet governance issues.

NTIA Must Not Be The "Court of Last Resort" For ICANN. When people are unhappy with ICANN, or with potential ICANN decisions, they go to NTIA. NTIA continues to maintain it doesn't oversee ICANN. But because NTIA has the power to do so, and because NTIA is the U.S. representative to the GAC, it will continue to attract the attention of parties unhappy with ICANN.

NTIA should give serious consideration to eliminating its "veto right" over ICANN and content itself with the MoU renewal as a means of maintaining suitable oversight to safeguard U.S. interests. In addition, NTIA should either transfer the MoU to some other agency, or should delegate representation to the GAC to some other agency.

Appoint someone other than NTIA to represent the U.S. in the GAC. As illustrated by the controversy over the proposed .XXX TLD NTIA's continued involvement in ICANN as U.S. representative to the GAC while simultaneously exercising oversight creates significant concern about the nature of NTIA's oversight. There is no reason why the same agency must both manage the ICANN MoU while representing U.S. interests. Transferring the U.S. GAC representation to another agency, such as the State Department, could eliminate this needless source of tension.

Let me stress that, as an American citizen, I feel that the current arrangement hampers the U.S.'s ability to represent me and my interests in ICANN. The U.S. needs a GAC representative that can forcefully represent U.S. interests without raising the specter that the U.S. is "really" sending a signal about what it will or will not permit. NTIA

representation of U.S. interest in the GAC, while simultaneously holding the MoU, is a historic artifact we should end.

NTIA Must Clarify When It Will Transfer Full Control to ICANN or Stop Pretending. In 1997, the United States proposed fully internationalizing the DNS under private sector management. In 1998, when NTIA picked ICANN to manage the root, it again promised to relinquish control over the root. Since then, however, NTIA has not explained when or under what circumstances it will carry out this promise to relinquish U.S. control. The "sense of Congress" resolution passed last year in response to pressure from WSIS strongly suggests that United States will never entirely relinquish control of the domain name system.

Bluntly, nobody likes a tease. If complete elimination of U.S. oversight of the Root is out of the question, NTIA should say so up front. We can have an honest and productive dialog with other countries on how to address real concerns about the U.S. role in DNS management if we delineate the boundaries of that conversation clearly. We cannot have productive dialog if it is premised on the assumption that we would some day accede to relinquishing all control of the DNS when we have no intention of ever doing so.

By contrast, if there are conditions under which the United States would feel comfortable relinquishing its current level of control, we should clarify what those conditions are and how ICANN can satisfy them. A clear set of milestones that ICANN must meet can provide a valuable road map and incentive for ICANN to reform itself. But NTIA should not commit to such a path unless it has confidence that it could, in fact, relinquish control under proper circumstances.

Recognize that ccTLDs raise sensitive issues. As countries increasingly rely on their country code top level domains for commerce and communication, they become understandably nervous about exercising control over them. Sensitivity is further increased by the growing perception that a ccTLD is as much an attendant right of sovereignty (or, at least, recognition as a distinct economy) as the right to participate in the Olympics or have one's own area code.

The United States would not be happy if the .us ccTLD were controlled by another country, even an allied country with whom we enjoyed close relations. The United States needs to find some way to satisfy other countries that it will not make unilateral changes to the ccTLD of a sovereign nation without the consent of that country's government.

Addressing ICANN's Real Problems

I have remarked in the past that ICANN recapitulates the FCC, but does it badly. ICANN has its own version of tariffing and price caps (for name registrations), its own version of license renewal hearings, complete with "beauty contest" style comparative hearings. In place of a "public interest" standard, it operates under a rubric of stability and consensus of the "internet community."

Sadly, with great power has come no responsibility. ICANN lacks a Congress or D.C. Circuit Court of Appeals to ensure that its decisions are not arbitrary, capricious or contrary to law. Its Board of Directors, the equivalent of the FCC Commissioners (whose open meetings and written opinions increasingly come to resemble FCC opinions, with concurring statements and dissents), serve as volunteers on a part time basis. This gives enormous latitude to ICANN's full time professional staff to set policy through contract negotiation with the entities ICANN regulates and through the recommendations to Directors that Directors have neither the time nor expertise to consider.

The question is not whether ICANN directors or staff are good people trying their best to do what's right in the world. On the contrary, I believe they are good people trying to do their best in an impossible job. The job is "impossible" because ICANN as currently constituted either does too much or too little. ICANN either needs to jettison its regulatory functions or complete its transformation into a regulatory body capable of

regulating properly. Since the former is impossible at this point, I suggest developing ways to do the later.

Two things make it impossible for ICANN to reduce itself to the narrowly focused non-regulatory body it wants to be. First, voluntary coordination of the kind envisioned by ICANN's founders and modeled on such entities as the Internet Engineering Task Force (IETF) worked because it they were ***voluntary***. No one needed to follow a standard set by the IETF, or get permission from IETF first before writing code. Once participation in ICANN became mandatory for inclusion in DNS, and once ICANN decisions became as binding as agency regulations, the entire dynamic changed.

Second, although ICANN publicly maintains that it has no intention of managing "internet governance," its commendably narrow focus became laughable as soon as ICANN also became responsible for protecting trademark rights. There is nothing remotely technical about using control over the Domain Name System to resolve complaints about whether this name or that name conflicts with a trademark. There is nothing technical about requiring would be registrars to have "sunrise" periods in which trademark holders can register names in the new registry before anyone else.

As ICANN has discovered, doing a little bit of policy is like the old cliche about being a little bit pregnant. ICANN now finds itself bedeviled by a non-stop stream of requests to resolve this issue or that. Law enforcement agencies want changes in how registries manage the "Whois" database to facilitate law enforcement – a move opposed by civil liberties organizations concerned with privacy issues and protecting speakers from retaliation by oppressive governments. After all, if ICANN can resolve problems for intellectual property holders, why can't it resolve problems for law enforcement or anyone else?

To illustrate by analogy, phone numbers in the United States are administered by the FCC as part of an international system called the North American Numbering Plan (NANP). NANP is a voluntary coordination between 19 different North American countries administered by a private company (Neustar). It works without fuss because each country maintains control of its own phone numbers and Neustar plays a ministerial role in facilitating coordination between the countries.

If countries participating in NANP decided to use it to take phone numbers away from people, required every government to pass through binding contracts to each phone number user to abide by conditions set via the NANP, or otherwise leveraged control of phone numbers, you can imagine it would attract quite a bit of interest all of a sudden. If those opposed to indecent speech over the telephone thought they could circumvent the Supreme Court's decisions protecting "dial-a-porn" by having NANP include a "voluntary" provision in every phone number agreement, they would show up to lobby NANP. So would those opposed to hate speech or other "inappropriate content." And with them would come those opposing such new regulation, or seeking additional regulation.

Even when avoiding such clearly non-technical concerns as trademark enforcement, ICANN finds itself involved in traditional competition and industry regulation questions that have nothing to do with technical stability. For example, to promote competition in the domain name registration business, ICANN required that TLD registries be artificially separated from businesses that register domain names (registrars). This may have made good economic sense (a debatable point), but it did not increase technical stability. To the contrary, it introduced an entirely new set of coordination issues tied to this split between the purchase of a domain name by a consumer and the actual registration of that name in the registry database.

One competition/consumer protection decision begets another. At the time Verisign and ICANN entered into an agreement in 1999, they set the "wholesale" rate for .com registrations (what Verisign charges registrars) at $6/name. No economic justification for this figure has ever been given. It was what ICANN and Verisign (and NTIA) agreed to

in private negotiations. The recent agreement between Verisign and ICANN renewing Verisign's control of .com for another 6 years would allow Verisign to raise the wholesale rate by 7% per year in four of the six years. Unsurprisingly, registrars have protested the decision.

Is 7% justified? Is it too much? Not enough? This is a classic tariffing question in rate-controlled industries. But ICANN has no process or expertise for setting or challenging a price. The process of rate setting, which impacts millions of .com registrants around the globe, takes place in private between staff for ICANN and staff for Verisign.

Meanwhile, other registry contracts raise new questions. Is it fair to treat .com and .net differently, because they remain the dominant registries? Recently, ICANN announced that it will permit new registries to have "variable pricing" under which a registry can set a different rate for a specific domain name or class of names, or could raise the price of a domain name after a registrant has invested in significant resources in creating good will in the name.

This has understandably created concerns. Some names may appear intrinsically valuable, such as "wine.com" or "sex.com." But should registries be the ones to capture that value? After all, the right to run a registry is a valuable license handed out by ICANN on an exclusive basis. Does it constitute an "unjust enrichment" to allow a registry to profit in such a way? By contrast, why should whoever proved lucky enough to register "wine.com" first enjoy all of the benefit? Why shouldn't the registry, which is creating value by creating the registry, be allowed to price its registration services under free market principles?

Worse, what about name renewals? The name "mediaaccess.org" had no particular value when MAP registered it. But if the Public Interest Registry, which controls .org, announced that it was going to assess new fees or cancel the name, MAP would pay those fees. MAP would not pay because PIR was suddenly adding new value, but because switching to another name would prove far more costly. Should ICANN restrict such practices? Should it permit them in new registries, but not in the dominant gTLDs such as .com and .net?

Finally, as the Site Finder incident demonstrates, even technical questions about how new registry services impact stability raise non-technical concerns. When and how registries should be allowed to innovate cannot be resolved without balancing a host of economic and political questions.

Unfortunately, I have no prescription for ICANN's overall ills. It is simply too late to eliminate the Uniform Dispute Resolution Process (UDRP) and revert to an organization providing only voluntary technical coordination. Even if such an arrangement were in the feasible set (and I have no illusions on that score), UDRP has become too widespread and imbedded in the web of contracts governing the DNS. And, even if UDRP were eliminated, the competition issues would remain.

If it is impossible to pare back ICANN to a non-regulatory body, then it needs to become a regulatory body that actually works. ICANN ending up as the FCC for the internet is pretty dreadful, but it beats ICANN becoming the equivalent of the International Olympic Committee or some other wholly unaccountable behemoth.

As numerous individuals, organizations, and academics have repeated time and again, ICANN cannot function without legitimacy. To gain legitimacy, it needs accountability. It gains these by having straightforward, transparent processes and some oversight authority that ensures that ICANN decisions do not exceed ICANN's mandate and that ICANN decisions have at least some rational basis to them.

ICANN also gains legitimacy by providing some means by which participants feel they are represented in the decision making process, and that participation in the process can have impact. While I do not suggest that ICANN must fulfill its 1998 promise to permit election of directors by internet users, it needs something better than the current

processes that seeks to fit all possible interests into 6 "Constituencies" with no formal process for participation by individuals.

I have no neat solution to this problem either. But NTIA can at least attack the accountability and representation issues through the MoU renewal process without tampering with ICANN's internal deliberations on pending matters. The Internet Governance Project, a consortium of interested academics, has filed comments with NTIA providing recommendations on how NTIA can use the MoU process to address the accountability and representation problems.[4] I hope that NTIA gives these and other proposals serious consideration when addressing the MoU renewal.

CONCLUSION

In examining ICANN and internet governance, this Committee and NTIA cannot content themselves by asking whether ICANN as it exists today is better than ceding authority to the U.N. Of course it is. To set the question up in such a fashion ignores the real problems that have made even the U.N. an attractive alternative to ICANN to some parties.

Instead, Congress and the NTIA need to address a different question, can we turn ICANN into a non-issue? I believe it is possible to do so by refocusing the broader debate on "internet governance" in an appropriate forum (the IGF) and getting ICANN to function in a way that stakeholders find acceptable. This last creates very real challenges for NTIA, particularly in light of the desire to shift "internet governance" questions away from ICANN. But failure to get ICANN to work in an accountable and representative manner will make it impossible to refocus the "internet governance" question. As long as ICANN remains both unaccountable and unconstrained, it will continue to attract parties looking for ICANN to solve its problems.

MR. BOHANNON. Chairman Upton, Chairman Stearns, members of the subcommittee, I appreciate being able to testify here today on the important role that ICANN plays in promoting confidence and stability on the Internet.

As the principal and the largest trade association of software and digital information companies, we have supported and carefully monitored the role and activities by ICANN since its inception, and we have seen firsthand how ICANN's policies contribute directly, as Chairman Stearns alluded to, combating online copyright and trademark infringement, promoting civil protection, combating cyber squatting, phishing, criminal acts on the Internet, including the pernicious effects of spyware. And those are all detailed in my testimony, I am not going to repeat them here.

ICANN plays that critical role because it sets the policy for domain names and IP addresses and the "Whois" databases. And that database and that information has been accessible to the public since the very inception of the Domain Name System.

As we are focused here at the end of the month on the renewal of the MOU, it is our view--and I think the view is held widely by others in my industry and others--that the focus needs to be on the Department of

[4]Available at http://internetgovernance.org/pdf/NTIAcomments-IGP-FINAL.pdf.

Commerce's future relationship with ICANN, and not entertaining speculative ideas about new entities or wholly new arrangements. Our belief is that it is vitally important that when the MOU is renewed, that the contractual obligations between ICANN and domain name registrars and registrees be fully and vigorously enforced.

More concrete steps need to be taken to improve the accuracy of contact data in the "Whois" database, and ICANN should commit to the preservation of public access to "Whois" data so that its many beneficial uses can be maintained.

For that very reason, last week SIIA and others joined with other trade associations, companies and other nonprofit groups in sectors ranging from banking, hotel, entertainment, online retail, technology and others to communicate this message to Mr. Gutierrez. And Mr. Chairman, I would ask that in addition to my testimony, this letter be introduced into the record.

MR. UPTON. Without objection.

[The information follows:]

September 13, 2006

The Honorable Carlos M. Gutierrez
Secretary of Commerce
U.S. Department of Commerce
Mail Stop 61
1401 Constitution Avenue, N.W.
Washington, D.C. 20230

Re: Memorandum of Understanding with ICANN

Dear Mr. Secretary:

The undersigned organizations and companies write to underscore a critical factor in your consideration of the next steps in the relationship between the Department and the Internet Corporation for Assigned Names and Numbers (ICANN).

The existing Memorandum of Understanding (MOU) with your Department gives ICANN stewardship of a critical information resource that promotes accountability and transparency on the Internet: the Whois database of contact information on domain name registrants. The goals that are set for ICANN, in an extended MOU or similar charter, must include ensuring that public access to the Whois database in all "generic" Top Level Domains is maintained, and that the quality of data it contains is improved.

Whois data is essential to maintain accountability and transparency in electronic commerce. Millions of Internet users rely on Whois data every day. Consumers use Whois to know more about whom they are dealing with online. Parents use the data to look into who may be behind websites that their children visit. And law enforcement agencies use the database to investigate crimes, frauds, and identity theft carried out online.

The business community and major non-profit institutions also depend on ready, real-time access to Whois data for many purposes, including:

- to identify cybersquatters and others who are infringing on trademarks online ;
- to investigate those conducting piracy, product counterfeiting, online fraud or phishing schemes over the Internet;
- to prevent or limit damage to our customers or contributors who are victimized by online frauds that are facilitated by misleading registrations of domain names;
- to cooperate with law enforcement to protect consumers against a wide range of crimes and misconduct carried out online, including identity theft and other invasions of privacy.

Public access to Whois data is a long-standing feature of the Internet and predates the establishment of ICANN. ICANN's stewardship of Whois should be a critical factor in shaping the Department's future relationship with ICANN. In particular, the Department should evaluate whether ICANN has done enough to fulfill its obligations under the existing MOU to improve

the accuracy of Whois data, and to effectively audit compliance with the Whois-related obligations of domain name registrars and registries. We believe these tasks have not been completed and that their fulfillment should be a requirement of any extension of the MOU.

Recent steps within ICANN toward restricting public access to Whois threatened many of the legitimate, beneficial and pro-consumer uses of Whois data outlined above. We commend your Department and other federal agencies for their efforts to ensure that the full range of public policy concerns, including consumer protection, are thoroughly considered before any changes are made in the well-established policy of unrestricted public access to Whois data. We strongly believe that this principle must be enshrined in any extension of the MOU between your Department and ICANN.

Extension of the MOU raises several other issues critical for ICANN's future activities. A number of the signatories to this letter have stressed these concerns in their individual submissions in NTIA's public consultation process. We thank you in advance for your consideration of those submissions, as well as of our shared views regarding Whois, in the upcoming decisions of your department regarding ICANN.

Respectfully submitted,

Activision Publishing Inc.
American Heart Association
American Hotel & Lodging Association
American Intellectual Property Law Association
American Society of Composers, Authors and Publishers
AT&T Inc.
Best Western International, Inc.
BITS (Financial Services Roundtable)
Broadcast Music, Inc.
Business Software Alliance
eBay Inc.
Electronic Arts Inc.
Entertainment Software Association
Guest Services, Inc.
Hotel Consumer Protection Coalition
Hyatt Hotels Corporation
InterContinental Hotels Group
International AntiCounterfeiting Coalition
International Federation of the Phonographic Industry
International Trademark Association
JPMorgan Chase & Co.
MarkMonitor Inc.
Marriott International, Inc.
Metavante Corporation
Motion Picture Association of America
News Corporation
Recording Industry Association of America, Inc.

The Honorable Carlos Gutierrez
September 13, 2006
Page 3

Software & Information Industry Association
Starwood Hotels & Resorts Worldwide, Inc.
The Body Shop International Plc
The Walt Disney Company
Transamerica Corporation
VegasInsider.com, Inc.
Verizon Communications
Walgreen Co.
Wyndham Worldwide, Inc.

For further information, please contact:

Steven J. Metalitz
Partner
Mitchell Silberberg & Knupp LLP
2300 M Street, NW, Suite 800
Washington, DC 20037
Tel: (202) 973-8136
Fax: (202) 973-8110
E-mail: met@msk.com

cc: The Honorable John M. R. Kneuer
Acting Assistant Secretary for Communications and Information

1070073

MR. BOHANNON. The concerns in this letter, and others expressed earlier this year, were prompted when in the first step of a policy development process a vote was taken to narrow the purpose of the

"Whois" database. That narrower purpose would have basically covered only a very small proportion of the current critical uses of publicly available "Whois" data. And many of the ways that we have used that data to fight intellectual property infringement, fight phishing and fight online crime would basically be eviscerated if that policy proposal went forward.

The reaction, even at the beginning of this year, was just incredible. And even the American Red Cross expressed its concerns that the impact of this vote on its ability to shut down fraudulent fundraising sites, such as those that sprang up within hours after Hurricane Katrina that hit the Gulf Coast last year, would be very much impeded.

Do we think ICANN is listening? I think despite the earlier steps this year, we think that some progress is being made. There does appear to be some backing away from the concept that the only purpose of making contact data available is to resolve just simple technical problems, which, of course, flies in the face of the role of the "Whois" database since the inception of the Domain Name System.

We are certainly hopeful, and we certainly want to commend the leadership of the Department of Commerce, Acting Administrator Kneuer and his team, as well as FTC Commissioner Leibowitz, for stating in our view a very firm view of the U.S. Government about the role of the "Whois" database, both at the last ICANN meeting and otherwise publicly.

But preserving public access to "Whois" is just one issue. It is also essential that we dramatically improve the accuracy and the liability of the data that we find there, and that problem has been amply documented. In a study that the GAO released last December, it estimated that the "Whois" data, in over 5 million domain names in dot com, dot net, and dot org, is either obviously false, incomplete, or simply could not be found. This is simply too high a level of inaccuracy which undermines the value of this important tool for all users of the Internet.

This hearing comes at a critical juncture, two weeks now before the end of the current MOU, and the relationship of the U.S. Government and ICANN. In the last renewal of the MOU in 2003, ICANN pledged to take steps to improve the accuracy of "Whois" data. It promised to put into place an enhanced system for ensuring that domain name registrars and registrees live up to their contractual obligations, including keeping "Whois" data publicly accessible. While some steps have been taken, and we do want to acknowledge those, ICANN's own report shows that the system does not work and the steps that have been taken simply are not operating in the way they were designed to do.

And I think this boils down to a very simple challenge, which is that ICANN has consistently shied away from taking on the more difficult

task of requiring registrars and registrees to take some proactive steps, any proactive steps to verify the information they are collecting from those who want to register a domain name on the global TLDs.

So Mr. Chairman, we want to acknowledge and confirm the important role that ICANN plays in promoting stability and confidence. And while some suggest that this could be done by another organization, either intergovernmental or otherwise, with all due respect, we do not agree. We think the more appropriate thing is to focus on improving ICANN's role. Let's not start over.

And I will be glad to take any questions you may have.

[The prepared statement of Mark Bohannon follows:]

PREPARED STATEMENT OF MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, PUBLIC POLICY, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Mr. Chairmen, members of both Subcommittees, I appreciate this opportunity to appear before you today and testify on the important role of ICANN[1] and, in particular, the role that ICANN plays in promoting stability and confidence on the Internet.

As the principal trade association of the software and digital information industry,[2] the Software & Information Industry Association (SIIA) has supported and carefully monitored the role of ICANN for several years. This has included active participation in the Coalition for Online Accountability (COA), which consists of many leaders in the copyright industry.[3] COA's goal is to enhance and strengthen online transparency and accountability. 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 ICANN's policies contribute to combating online copyright and trademark infringement, consumer protection, cybersquatting, phishing, and other fraudulent or criminal acts online, including the pernicious effects of spyware.

---

[1] The Internet Corporation for Assigned Names and Numbers.

[2] 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.

[3] 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.

As a private, bottom-up organization that represents the interests of all Internet users, ICANN's role in this area is of utmost importance. This is because ICANN sets the policies for domain names and IP addresses in the Whois databases.[4] Whois data has been accessible to the public since the inception of the domain name system. Since 1999, ICANN has been assigned this function. 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.

ICANN's Memorandum of Understanding with the US Commerce Department -- which provides, to a great extent, ICANN's charter for management of the domain name system -- expires September 30. It is our view that the focus should be on DOC's future relationship with ICANN -- and not on speculative ideas about new entities or wholly new arrangements. In whatever form the DOC-ICANN relationship takes, SIIA believes that it is vitally important that the contractual obligations between ICANN and domain name registrars and registries be fully and vigorously enforced. More concrete steps must be taken to improve the accuracy of contact data in the Whois database. And ICANN should commit to the preservation of public access to Whois data, so that its many beneficial uses can be maintained. Last week, we joined with 35 other trade

[4] "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.

associations, companies and major non-profit groups to communicate this message to Secretary Gutierrez, in a letter which I attach to my testimony and ask to be included in the record of this hearing.

The Importance of an Accurate, Complete and Accessible Whois

As you are well aware, Mr. Chairmen, 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 explained on numerous occasions, 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,[5] and the Center for Democracy and Technology has found the Whois Database a critical tool in bringing their high profile complaints against spyware distributors and educating consumers on the pernicious effects of harmful downloads.[6]
- **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,

---

[5] 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.")

[6] 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).

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."

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. 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.[7]

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

[7] 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 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."

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.[8] Just last week, a wide range of companies and entities – financial services, consumer retail, software, movie, auctions, hotel and lodging – wrote to Commerce Secretary Guttierez indicating the critical role of Whois data and asking that the current policy be preserved and improved upon.

Finally, 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

[8] 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 adverse impact on transparency and accountability online.

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.[9] 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

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

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. 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

ICANN plays an essential role in promoting the stability and confidence that all users have in the Internet. Some suggest that this could be done by another organization, perhaps by an intergovernmental organization. With all due respect, we do not agree.

We believe that it is appropriate to focus on improving ICANN's role – not starting over. 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.

MR. UPTON. Well, thank you. And I certainly agree with your closing statement that we want to improve what we have today. And I

just want to say before I start, because we are expecting votes on the House floor soon, if we do this right and maintain a tough gavel, I think we might be able to get all our questions in before the votes start. But I want to thank and commend Kelly Cole, our diligent staffer; this is the last hearing that she will be on this side of the dais. And she has been worth her weight in gold, and she is off to greener pastures--I get an extra two minutes, right, Kelly?

MR. STEARNS. Mr. Chairman, I will just say a few words also. Kelly has helped me on my subcommittee, so I also want to congratulate her in her transition.

And when a person takes her last night in an Air Force airplane, what they do is all the crew douses that person with water, but we won't do that with Kelly; we won't give her that cold chill, we will give her the warmest greetings as she leaves.

MR. UPTON. We will save that for Coach Carr after he beats Wisconsin this weekend.

Okay, the clock has started.

Thank you all for your testimony. And again, Mr. Bohannon, I certainly agree, how can we improve this process? I don't think anybody here on this panel wants to see the U.N. put out their air balls and exert a great influence on the process. But I will tell you, the question that comes to mind right away for me is, obviously, the story that broke this week that the MOU is going to be extended. There weren't a lot of details that were given, but I would note that that is yesterday's news.

The 30th is next week, and I am just wondering what details the two of you might be able to give us in terms of how long an MOU we are expecting? What changes do you see, particularly in light of some of the testimony by the other four panelists, in terms of how can we improve the system. What light can you shed on the process today? And remember, you are not under oath, so you can tell us. No bad consequences will happen.

MR. KNEUER. Oath or no oath, I will be truthful.

Yesterday, at a hearing at the Senate Commerce Committee, I was asked this question, will there be an extension of the MOU, and the plain answer is yes, we intend to extend our Memorandum of Understanding with ICANN to help continue this transition. Each Memorandum of Understanding that we have executed with ICANN has been publicly available on the Internet, and I am sure this will be no exception. We conducted this consultation over the summer to look at how has ICANN progressed through the last version of the MOU? What are the issues that are most outstanding? And I think the comments we have heard of the panel this afternoon reflect very similar issues to things that we heard.

MR. UPTON. And let me interrupt you for one second. I would guess that all four of you submitted comments, right? You are among the 700 that they reviewed; is that right? Anybody not submit comments? Mr. Feld. Two, Mr. Lenard and Mr. Feld did not submit comments. Okay. Go ahead, I am sorry.

MR. KNEUER. Clearly the areas that people had continued concerns are transparency and accountability. Over the last iterations of the MoU, the progress that ICANN was making was largely institutional, organizational, getting staff in place, having budgets in place, having contingency plans, those sorts of things. That being said--and they have made enormous progress in that regard--that being said, the ultimate goal of having a lasting institution that has well understood and well articulated processes in place for accountability and transparency is ongoing.

And those are the sorts of things that I believe that we expect to memorialize in our ongoing agreement so that we can continue this transition, that we can have in place an institution that we all collectively have confidence in, that it will be lasting and stable and secure and will be able to carry out this function with the confidence of its constituents.

MR. UPTON. For how long?

MR. KNEUER. In the past, we have done these for 1 year, for 3 years. I think what we want to be mindful of is give it enough time that they can actually make progress, we don't want it to be so short in time that nothing realistically can be accomplished; but at the same time, we don't want it to be so long that it appears to be interminable. So those are the sorts of things that we are still discussing, but I would imagine it would be somewhere in those sorts of timeframes that we have had in the past.

MR. UPTON. Probably at least 3 to 4 years?

MR. KNEUER. I think 4 would be longer than anything we have done in the past, the last one was 3. But I think they have made significant progress, so I think we can look for a timeframe that, as I said, gives them an opportunity to get some real concrete work done, but is not so long as to--and also recognizes the fact that they have made considerable progress--this process has been going on for an extended period of time--something that indicates a clear path forward.

MR. UPTON. You didn't tell us a lot in terms of details.

Dr. Twomey, can you tell us a little more? Knowing that you came the farthest, right? Didn't you come from halfway around the world for this?

DR. TWOMEY. Actually, in some sort of bizarre post Cold War phenomenon, I flew in from Moscow to attend, being in some key conferences there.

Chairman, part of my response would be that we are having these hearings today, not on the 30th, and so this discussion is clearly underway. But I wanted to reinforce what Mr. Kneuer has said. ICANN has achieved, I think, a lot in the last 3 years in terms of the many things in the existing Memorandum of Understanding for organizational development and strength and what have you. Part of its commitment going forward is also that it takes much more of its own sense of control, a sense of its own purpose, a sense of its own destiny if you like. I make that point because the board itself is considering a new set of principles for private-sector management and operating principles which are directed to many of the things that members have actually pointed out. The board itself has been listening very closely to the feedback from members of the community over the last 18 months, and things like transparency, things like high standards for accountability and other issues are very important to the board.

I did make the point in my opening statement that I think there is a lot of transparency in what ICANN does, but it needs to maintain the various high standards, and the board is committed to that. Separate to any discussion in an MOU, the board itself is working on a set of principles in response to what it has heard from the community to direct where it goes directly towards these things. In other words, it doesn't need the United States Department of Commerce or anybody else to tell them what it needs to do to achieve its task, it listens to its community and is really working on that.

But we have also been in discussions about the nature of the sort of relationship we need to go. We recognize and value the role that the Department of Commerce has played in the MOU process in due diligence about the growing sense of ICANN and the development of this form of Internet governance, if you like. And we do recognize that we will have some arrangement going forward; I think it will be of a slightly different nature in the detail than the previous ones.

And the timeframe I think is something that we are also still considering. I couldn't give a straight answer on that, the consultation of the board is still underway. But we recognize the things that have been put forward in the consultation process, in the consultation process that we have taken, we think they are important. But a lot of those things I think that we, as a board, just want to do ourselves.

MR. KNEUER. Mr. Chairman, if I could just add to that, saying that I didn't give much information. We will have all the information when we are done.

MR. UPTON. Okay. Ms. Eshoo.

MS. ESHOO. Thank you, Mr. Chairman.

I have two questions--well, I have lots of questions, but I don't have a lot of time and the bells are going off.

There are two questions, and I want to direct them to Mr. Twomey, but I want to thank the entire panel for your testimony and your work, some I know and have worked very closely with.

And Mr. Feld, I am glad that you are here today. You have a lot on your mind, and it has been building up over 5 years I think, right? I am not diminishing it, really, but thank you to everyone.

So to Dr. Twomey, I have heard--and I have made references to this--complaints about ICANN's lack of transparency. Transparency is a big word, you know, and a lot of things can come under that umbrella. But particularly with regard to the contracting processes and the ability of affected parties and the public to provide input into these important agreements. And there is a protection of the contract. VeriSign has a contract; they are proud of the work that they have done. But, you know, the mark of humanity is that no one is perfect. No matter what it is, no matter how hard we work to refine things and recognize, it is like punching a pillow, you put a dent in it and there is something else that comes up.

My sense is is that the way the system works is that you really don't have to pay very much attention to complaints. And that is my sense from what I have gathered. So tell me what you and your contractors are doing to provide the best service possible. And, in particular, are you using technology to handle these things? You make reference in your testimony to how many things are posted and whatever, but I don't know if that really speaks to it, you know?

And my other question is, and you touched on the London School of Economics, but they issued their report on your GNSO, and the report says that that the GNSO must have greater transparency and enhance its ability to reach consensus positions, and that you have to respond much more quickly--I think the "much" was underlined--to your constituents. So what are you doing about these recommendations?

DR. TWOMEY. Good set of questions, Congresswoman.

Come to the first one, your point about transparency, it is quite--you are right, this is a very difficult topic. I think our processes around these contracts, in particular, where there has been feedback on the sense of not being transparent. These contracts have been out publicly, they have been posted.

MS. ESHOO. Well, if I might. It is one thing to be able to read the language of a contract, it is another thing to be able to go somewhere and talk to someone about it. It is not just reading something.

DR. TWOMEY. I agree with you. But this is my point, I was saying about accessibility. I think one of the things we need to work more on is

it is not just a question of having this material posted, but you have to make it more accessible for people to understand.

MS. ESHOO. So if I have a complaint about it and I send something to you, how do you handle it?

DR. TWOMEY. Well, we have two ways of handling the complaints. First of all, there are complaints handled through staff processes, but we also have an independent ombudsman, and if people have future complaints they can take those complaints to the independent ombudsman.

MS. ESHOO. Do you have backlogs on it? Are you all up to date? Does anyone ever meet with anyone, with organizations?

DR. TWOMEY. Yes. We have a process of meeting with people throughout the year, but we also hold three very large public meetings a year where member constituencies all come together. The ombudsman, for example, is available the entire time there, he has an office available for people to come and talk, staff and board members and others as well. I mean, we could keep--

MS. ESHOO. Well, see, I think that there is a lot of quality and a lot of important growth and management and all of that, the organization. I think you have a ways to go. You know what we call it? Constituent service. And you know what? None of us would be sitting up here unless we really gave good constituent service because they are not so much into how we voted on the previous question, but rather how we have responded effectively to what people are saying to us.

DR. TWOMEY. I would agree completely, and we are looking to dedicate more resources on this. But I think as you, in Congress, would know more than most--more than all, really--you can have open transparent processes, you can go through a set of feedback, eventually you have to make some decisions as a board, and often people who don't like the decision will often criticize your own process.

MS. ESHOO. Well, if that is where you start from, it is going to affect your process. What about the London School of Economics?

DR. TWOMEY. Their review process has just been made public; they just finished their independent review. And members of the board and of the Generic Names Supporting Organization's own constituencies are now coming together as to how to actually implement some of those recommendations and discuss those recommendations.

So the response there will be bottom up, it won't be from myself or the board down saying this is the answer. We will be listening to further consultations on those recommendations.

MS. ESHOO. Who is going to consult with you on them? They are?

DR. TWOMEY. They have given this report to our community. Our Generic Names Supporting Organization and the board are going to

convene a process for handling that report and figuring what the way to respond to it should be. Again, it will have to be through an open consultation process.

MS. ESHOO. It seems like if you could have a more direct punch to what you do, but that is just my observation.

Thank you, Mr. Chairman.

MR. UPTON. The Chair recognizes Chairman Stearns and will just announce votes have started in the House, Mr. Stearns will continue to chair.

MR. STEARNS. [Presiding.] Thank you, my colleague. I am going to get through my 5 minutes.

And Mr. DelBianco, this is a question for you. Is there a threat in letting ICANN go independent too early, that would open it up to a takeover by another body such as the United Nations? Just yes or no.

MR. DELBIANCO. The answer is yes, Mr. Chairman.

MR. STEARNS. Okay. Can governance be separated from the technical functions of integrity and availability when both are necessary to address certain cyber crimes?

MR. DELBIANCO. Cannot be separated. We need to do all--we need to do availability and integrity. And not just as ICANN as manager, the FTCs and the similar FTCs in other nations also have to participate in protecting consumers.

MR. STEARNS. How do we do that? How do we get the nations to participate?

MR. DELBIANCO. We cannot convince other nations to legislate in the same way we do on consumer crimes, on spam, on spyware and on regulating of content. All we can do is expect them to respect our wishes to cooperate in law enforcement efforts, and that is one of the key reasons that the "Whois" data has got to be open and accurate. As Chairman Leibowitz said yesterday, if the FTC had to go into another nation and beg a registrar there to provide the information needed to investigate a fraudulent website, they would have very little to stand on if ICANN were not enforcing the accuracy of the "Whois" database.

MR. STEARNS. Do you think we have to develop a cross-border fraud bill in the United States that would have some accountability and have some way to enforce it?

MR. DELBIANCO. I think the chances to do that on fraud are far better than the chances to do it on content regulation. We will have too many differences when it comes to content or censorship, but on fraud I think it is promising.

MR. STEARNS. Do you think we should try to pursue then today this cross border fraud, on the fraud, but leave the content to a later date then?

MR. DELBIANCO. Yes, Mr. Chairman.

MR. UPTON. Do you think there is any hope to ever do any in content, or is it just because there are so many cultural challenges here that--I guess we can't.

What is the biggest threat of the Internet if the abuse of domain name practices are not stopped?

MR. DELBIANCO. As the integrity of being able to get to the Internet website you originally intended begins to erode, businesses lose their ability to control the consumer experience, consumers begin then to lose confidence that that site hasn't been redirected or that is not a fraudulent website. It will have an ancillary effect as well, because advertisers--and again, advertising revenue really drives a lot of what happens on the Internet today--advertisers will lose the effectiveness of their impressions if fewer and fewer of them are reaching the target audience they were intended for.

MR. STEARNS. Mr. Lenard, you state that ICANN has had a relatively light touch. What do you think a multi-lateral organization, if they were put in charge of the Internet, is likely to do, perhaps in terms of regulation or that type of thing?

MR. LENARD. Well, obviously, one can hypothesize, but first of all, other nations --for all the regulation we sometimes don't want that we get here--other nations just have a much more regulatory approach, many of them less faith in the free market. And I think you would have lots of kind of what we would call rent seeking behavior, behavior between various countries trying to use the procedures to try to gain competitive advantages for themselves, and I think that would be ultimately quite damaging.

MR. STEARNS. If we want to promote innovation and investment by the competing registry operators and reduce regulation, do we invite a greater threat from those who want a multilateral organization to control the Internet?

MR. LENARD. No, I don't think so. I think we need to have pro-competitive policy. ICANN needs to have as pro-competitive a policy as possible, that will stimulate investment. And I don't think that necessarily will invite, you know, more interest in a multilateral organization.

MR. STEARNS. Mr. Bohannon, how do consumers benefit from the "Whois" database, and does it apply to entities outside the United States?

MR. BOHANNON. Thank you, Mr. Chairman.

Let me answer the second part first. The "Whois" database supplies right now to all the domain names registered in any of the generic top level domains, dot com, dot net, dot org, et cetera. There are separate

"Whois" databases for all the country code TLDs, and that is not really the subject of what my testimony was about.

Consumers benefit because, quite frankly, when they get an e-mail that looks like it is legit, they can go check out the domain name, verify independently who it is that they are dealing business with. And when they submit a complaint to a consumer protection authority, whether it be the Attorney General or the FTC, the FTC can do the same thing, it can help identify whether, in fact, it came from a legitimate source or not.

MR. STEARNS. How does fraud affect your members and their ability to conduct business, consumers and other businesses who want it?

MR. BOHANNON. It occurs a number of ways. My testimony outlines that certainly for our industry, the ability to go after pirates of our intellectual properties is absolutely four square in the interest of our members and something that we are daily in the role of working together to try to figure out how we go after this.

But my members, many of whom are well known brands, are also the victims themselves of phishing attacks to their consumers who claim that they are representing a product--people out there representing that their products are a certain company's product, which is not true. So both on the side of protecting intellectual property, as well as combating fraud and phishing, my members need to make sure that the system by which we can know who we are doing business with is both something we can rely on, that it is accurate and up to date, and that we have the tools to use it freely and in real-time.

MR. STEARNS. Can fraudulent websites be detected or prevented with tools other than "Whois" database?

MR. BOHANNON. We have never said that the "Whois" database is the silver bullet, but we are not aware of any effort to go after either an intellectual property pirate or a scam artist that doesn't first use "Whois". Once you have that kind of information, you can then use other tools, both technology, legal self-help. But we are not aware of anything that doesn't first require us going to the "Whois" database to double check where it is.

MR. STEARNS. The subcommittee is going to temporarily adjourn until we vote, and we will be back. There are several other members that wish to ask, so we appreciate your forbearance.

[Recess.]

MR. STEARNS. The subcommittee will come to order. And Mr. Green is recognized.

MR. GREEN. Thank you, Mr. Chairman. And I would like to ask unanimous consent for my statement to be placed into the record.

MR. STEARNS. By unanimous consent, so ordered.

[The information follows:]

PREPARED STATEMENT OF THE HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Thank you to our Chairman and Ranking Member for holding this hearing on the Internet Corporation for Assigned Names and Numbers or ICANN.

The Internet is a unique asset that poses many challenges for individual nations to manage individually and collectively.

The United States government, including actions by Congress, helped create the Internet, but it is now a huge international system of networks that defies complete control by any particular government.

Comparing the problems of unwanted email and telemarketing solicitations proves that the Internet is beyond even the control of the United States, the most powerful nation on earth.

While our federal law is an extremely important tool against spam, it can never work as well as the do-not-call list because the problem requires major international cooperation.

As a result, the question of how to coordinate the technical and management aspects necessary for the Internet to work is also extremely important.

An effectively functioning Internet is clearly in the national interest, and removing these functions to the United Nations is a bad idea.

The United Nations is a diplomatic body for debating international issues, and is not a particularly effective standard-setting or management agency.

In addition, there is a lot of anti-American sentiment around the world these days and a U.N.-managed Internet governance body would likely see spill-over from other diplomatic disputes.

Even if the U.S. Department of Commerce limits their impact on ICANN under the current arrangement, the appearance of control inevitably makes America a target of some criticism.

As a result, it may be difficult to continue forever with the appearance of American control over ICANN, because at the end of the day the Internet is global.

I look forward to learning more about these issues from today's hearing and questioning our witnesses on some of the recent controversial with ICANN.

In particular I am interested in their proposals to remove the "Whois" database of website operators from the public domain and the recent settlement with Verisign.

Thank you and I yield back the balance of my time.

MR. GREEN. Mr. Twomey, in a Senate hearing yesterday, there was a discussion that ICANN consider, change, or restrict the access to the "Whois" database of website operators, and it is currently publicly available on the Internet. Both the FCC and FTC and other U.S. and international law enforcement agencies are concerned of this move because it restricts ability to stop spam, spyware and identity theft. Our office used this database before to find out who registered websites in my own name, and our FTC Commissioner Liebowitz said that the FTC uses database in almost all its Internet investigations and seems very worried about ICANN's new policy.

During our work on our spam bill a few years ago, I learned it is difficult enough to police the Internet and prevent spam, spyware,

identity theft and viruses without introducing more hurdles to law enforcement.

If ICANN goes forward with the change and restricts access to "Whois" database, what would the FTC and other agencies do, much less the Members of Congress who want to know who is using--has an Internet address with our name on it? And how would it be able to access that information?

DR. TWOMEY. Thank you, Congressman, for the question.

Let me be clear about where we are with "Whois". ICANN's policy on "Whois", as it presently stands, is quite clear, to maintain timely, unrestricted public access to accurate and complete "Whois" data, including registrant technical, billing, and administrative contact information. And that is our policy, and that is what is written into our contract. So that is what we administer and enforce and will continue to enforce.

MR. GREEN. So it will be available?

DR. TWOMEY. Yes. And we are putting more resources into that.

We have a policy development process, which is a bottom up process, and "Whois" has been in a discussion in that arena for some time. And the points that have been referred to in the Senate yesterday and other places has been some discussion by some constituencies about changing that policy. But that policy cannot change without input from all our constituencies, including all of the governments who are part of that process, and many others. That could take a very long time, it may come to nothing at all. And the sentiments that you have put forward and others put forward are clearly going to be heard in any crisis. And at that stage, you know--because it is being discussed, it does not mean that is what ICANN is going to do.

MR. GREEN. We have that problem here in Congress.

Mr. Kneuer, do you have anything else to add to this?

MR. KNEUER. Other than that it is the express position of the administration, not just in the Department of Commerce, but across all of the various executive branch agencies and equities that have an interest in "Whois" database that is publicly available, accurate and searchable "Whois" information is critical for law enforcement for the protection of intellectual property and others. We think it is vitally important that ICANN enforce its contracts to ensure that that information is made publicly available. We have made our input into the government advisory process, and we will certainly be active in all of ICANN's processes and elsewhere to make sure that information remains publicly available, accurate and accessible and searchable.

MR. GREEN. My next question for both of you today is that, under the recent litigation settlement between ICANN and VeriSign allowed

VeriSign to increase prices for domain names 7 percent per year, 4 out of the 6 years. One of the concerns I have about that is we are still working on when AT&T was a monopoly and the FTC controlled their cost, I know in settling lawsuits, is it just the settlement of the lawsuit, or is there a background reason for the 7 percent per year?

DR. TWOMEY. Congressman, you pointed out that contract, proposed contract coming out of a very broad settlement arrangement around a series of issues, and that particular term--which is just one of many, many terms in that contract--emerged out of those negotiations. And out of a sense from VeriSign, the things that they saw as being important, as they put it, the need to ensure sufficient funds for increasing demands in their infrastructure and infrastructure investment, particularly for security.

I would just make this observation, Congressman; under the previous contract, they also had the right to ask for a price increase.

MR. GREEN. Oh, I don't mind. I was just wondering 7 percent compared to 5 percent, or whatever.

DR. TWOMEY. That has been a matter, I think, of negotiation.

MR. DELBIANCO. Congressman, with respect to that, in May our group commissioned Zogby International to do a poll. They polled 1,200 American businesses who owned websites and asked that question, how much does this--well, 7 percent doesn't really tell the story, it is 1.86. For instance, on a domain name registration that costs between 10 and $50 a year, within the context of building and maintaining a website in the Commerce platform with technical support--it is irrelevant. And the survey results came back that 81 percent are completely unconcerned with 1.86, especially if it was presumably going for security and stability. They were far more concerned about those integrity problems we discussed.

MR. GREEN. Mr. Kneuer, is the Department of Commerce entered into the Memorandum of Understanding with ICANN on that settlement with VeriSign?

MR. KNEUER. We don't look at the overall settlement of the litigation with ICANN and VeriSign, but as part of that litigation settlement, they renegotiated the dot com registry agreement. As part of our overall management of the transition of the DNS to the private sector we have retained the right to review those contacts. We are reviewing the VeriSign-ICANN dot com registry agreement.

We are doing that in consultation with the Department of Justice, Antitrust Division for purposes of these competition issues and the pricing issues that you raised, as well as with various entities throughout the Federal government that have insight and expertise on matters of stability and security.

And if I just might, my experience with the Antitrust Division in this review is that they have been wide awake and very vigilant in their work on our behalf. They have been extraordinarily proactive and hardworking in their review and analysis; and we very, very much value the advice and the expertise that they provide us.

MR. GREEN. This is probably my last--I can't read how much time I have left, Mr. Chairman, with the lights, but did VeriSign commit that these funds would be used for the increased security?

DR. TWOMEY. There is no explicit terms in the contract to that effect. Their public statements have all been directed towards that effect. There is no requirement in this contract that they have to increase their prices, that is the other point. This doesn't say that there will be a price increase, it just doesn't label it.

MR. GREEN. Okay, thank you, Mr. Chairman.

MR. STEARNS. I thank the gentleman, Mr. Shimkus.

MR. SHIMKUS. I thank you, Mr. Chairman. And I appreciate you all being here. It is really noteworthy that we are finished voting today and members actually came back. I don't know if that is good or bad, but it does show you that there is interest by many of us to try to figure out and understand this, which is kind of a bizarre process. And it has been working, but I think people have questions, and that is why I am going to first start with Mr. DelBianco.

In your testimony, you note that you believe the authoritative or A root server belongs in the United States. It is currently located in Virginia, can you explain why you believe this?

MR. DELBIANCO. Thank you, Congressman.

I did suggest in there that I am echoing what I believe was a very strong statement by both the House and Senate last November, unanimous in both House and Senate, when they laid out a series of parameters around which the U.S. wanted to maintain oversight of the Internet. And one essential ingredient in that, unanimous in both Houses, was that the physical master copy, we will call it that, the master copy of the highest level table be physically kept in the United States. It is a security backstop. Not unlike the other things the U.S. has done by negotiating backup agreements with certain partners, contracting partners to make sure that whatever happens with ICANN, we can guarantee the stability and security of the DNS.

MR. SHIMKUS. Which is part of the issue on, you know--I concur with the analysis of what the legislative bodies did, but that is also part of--that is why NGIA is empowered with an oversight role. But I want the other panelists to comment on the same question.

Do you believe that the A root server--the A root should remain in the United States? And I don't know if you can comment, but whoever

would like to comment on that, I want to open it up for the panel. Go ahead.

MR. BOHANNON. Congressman, my association has not taken a formal view, but I can give you my personal, professional opinion based on my--

MR. SHIMKUS. I will take it.

MR. BOHANNON. Which is, I agree with Mr. DelBianco, I think it is the right thing to do. And I have yet to see any reasons or conditions that would lead me to believe that that policy should be changed any time in the near future.

MR. SHIMKUS. Mr. Feld.

MR. FELD. I would just say that this is one of the matters which actually should be the subject of some discussion with other governments. That may be the appropriate thing now. There may be other arrangements which would satisfy our concerns with regard to security, commerce and so forth, which would not involve the A root residing in the United States, and a gesture like that might well go a long way towards satisfying a number of concerns abroad.

MR. LENARD. I agree that it should be kept in the United States--for the present certainly.

MR. SHIMKUS. Let me--Mr. Feld, I find that a lot of the debate has been addressing--and I think Mr. DelBianco before, and in response to my friend from the Houston area, that what the entities who are using it want to make sure of is safety and security and the like. So you don't fear those issues, should the root server be moved to other countries?

MR. FELD. No, that is not what I said. What I did say, however, is that we have a global system; we are participating with other countries. ICANN strives to be a multinational organization, and one in which other countries feel that they have a genuine role.

A question as complex as where should the A root reside is one that I think we should be willing to think about. What is important, I think, is not just to conclude ourselves that this is the best place for it, and why would anybody want it elsewhere, but to think about, if we are concerned with making sure that other people buy into the notion that the United States is not trying to keep a privileged position for itself any more than necessary for Internet stability, that we need to be open to the possibility that there might be a reason to relocate it, and do so in a way that would still satisfy our concerns about security.

MR. SHIMKUS. Okay. I disagree, but I respect your opinion.

Mr. Lenard, did I cut you off? Did you have anything more to say?

MR. LENARD. I had actually finished. I was going to say I agree that it should be kept in the United States.

MR. SHIMKUS. Mr. Twomey.

DR. TWOMEY. Thank you, Mr. Congressman.

As far as--my understanding is there is no discussion, expectation--well, there is no discussion of this topic; there is no talk that I know of on that issue. But I wanted to make this point. Root servers have evolved of recent time, particularly utilizing a key technology called Anycast. And so what we now have is, instead of having what we used to have 13 pizza boxes, 13 root servers, we actually now have 13 clusters. And these are now distributed across 50 countries around the world, and this is growing significantly.

And I think that is a key part of how the technology evolves to keep--because I do agree with the international access, international aspect of how serving a billion users of the Internet around the world--150 million are Americans, but 50 million are not Americans. So I think the key thing here is that the technology takes away some of the symbolism because it is allowing us to actually ensure that root servers are distributed throughout the world and operated in big clusters.

MR. SHIMKUS. But does the movement of the root server, would that change the oversight of our Department of Commerce and NTIA?

MR. KNEUER. If I might, Congressman. This discussion of unilateral U.S. action and this concern over unilateral U.S. action, the unilateral action that we have taken--the only unilateral action that we have taken is the decision to take this critical government function and transition it into the private sector. We did that on our own initiative. Rather than keeping this authority forever enshrined in the U.S. Government, we took the unilateral step to start this transition into the private sector. The A root is essentially managed and run by the private sector. To move it because it might makes somebody else feel good makes zero sense. To introduce instability into the critical infrastructure with no technical justification of any kind doesn't make any sense at all.

MR. SHIMKUS. As long as the Chairman allows me to go over my time, Mr. Feld.

MR. FELD. If I may, as I stated in my testimony, as an American citizen and as a Senior Vice President for an organization that is concerned with freedom of expression, I am extraordinarily happy with having the United States maintain control of the A root and to maintain a level of oversight over the naming system. As I said at the beginning, I would find it extraordinarily troubling if we were to internationalize this and to move this out in an irresponsible manner.

At the same time, however, there is an enormous difference between a system in which we say we are working with the world because that is the appropriate thing to do--and this is a global Domain Name System--and to say we are working with the rest of the world as a matter of grace, but where we want to draw the line we choose to draw the line.

Every Nation, I think, would recognize that we are obviously going to protect our interests as we need to, but in a very complex negotiation among nations who are increasingly dependent upon this resource, I think it is a responsible thing for us to do to consider how we can protect our own interests, and at the same time ensure that those governments that are inclined to trust us and are not permanently dedicated to being against our interest feel that they have a measure of involvement and security.

I am not suggesting moving the A root, and I think that an attempt to do so now would be inappropriate; but I would prefer that at this stage, and as a general rule, that our policy would be that we set limits on the things we categorically take off the table unless we have to.

MR. SHIMKUS. Okay. And let me just, finally--I think the problem that the laymen--and I really admit that I am a laymen in this, I am not a techie, and I have tried to follow this for a while--is that there is really schizophrenia in this management control oversight, who pushes who, is it going to be--are we moving to a free market, in essence, competitive issues or are we still going to have oversight?

We want to move, but then we want to control--so let me ask you, Mr. Twomey, what steps are you taking--this is America, we like free market capitalism. We like, if there are competitive markets, for them to be fair. And thereare winners and losers, and those losers should be able to find out why they lost, especially in this quasi-government oversight process by which we empower the, in essence, the providing of business.

So what steps are you taking to increase competition in your spaces?

DR. TWOMEY. Well, I think the key aspect of competition has to be judged by the consumer. So I think one of the first questions in any discussion about competition is competition for whom? And we take respect of competition for registrants, and I think that is a key principle.

At the heart of that, therefore, has been, first of all, in the generic top level domains in which we have policy influence, a separation of the registry from the registrar; in other words, a separation from the databases from those who actually sell you the domain name, if I can make it as simple as that. That has resulted in the usual things you get. And in that separation, the registrar function is something that clearly can be open to competition and can be replicated. And we have gone from one registrar to over 800 now. The benefits of being what you get from that sort of competition, one, it is bidding price, so prices can be up to less than 90 percent of what they used to be.

The other benefit is the market increasingly implements new services, packages new services, there are registrar--

MR. SHIMKUS. Or promises of security issues? I mean, better quality, better--

DR. TWOMEY. That is right. Some registrars now package the domain name, but it is part of the package of services around hosting, around looking after your intellectual property interests and domain names. There is a whole series of things people offer.

When it comes to registries, the key point there is introducing more and more registries and more and more gTLD. And we are in the process, we have increased the number of gTLDs to 11 additional ones. And there is a policy process underway now to look at potentially opening up to full liberalization for new gTLDs, and a process for how we would actually introduce more gTLDs on an ongoing basis to give consumers again more choice of not only who they buy it from, but what TLD do they get?

MR. SHIMKUS. I think I understood that. Your acronyms--

DR. TWOMEY. Yes, I am sorry. The point is, it is not just dot com; you can get a dot net, you can get a dot org.

MR. SHIMKUS. Well, I know in the dot net issue, that was open to a competitive process, and we had--what are the results of that?

DR. TWOMEY. I understand. Let me take you where your question is going.

An important part of the process of moving to competition was a series of discussions that took place in 2000 and 2001 with the Department of Commerce, VeriSign and ICANN to further tease out what was VeriSign's dominant position on dot net, dot com, and dot org, three top level domains. And in the agreement that was done at that time, it was agreed that dot org would be rebid and VeriSign could not bid for it.

The dot net would be rebid, and VeriSign could be a bidder along with another people, and that dot com would not be rebid, it would be renewed. And that was a decision made in 2001.

It is an important point to your question because--

MR. SHIMKUS. I think it is important to lay the whole--I mean, that is why we have these hearings, to get the whole story of how you are moving, and hopefully in some progress towards these ends.

DR. TWOMEY. So we could rebid dot net last year under those terms and those agreements, and there was a price competition as you pointed out. Dot com, the board of ICANN, as it was constituted last year and this year, did not have the legal freedom to rebid dot com because these were agreements made in 2001, so we were already bound by agreements that were made in 2001 by the three parties.

MR. SHIMKUS. Thank you. I learned something, I appreciate it.

I yield back, Mr. Chairman.

MR. STEARNS. I thank the gentleman. I think I will close and just ask sort of a general question for Mr. Feld and Mr. Twomey.

As I understand it, decisions by ICAAN are made by a board of directors, they are really not political appointees, they are really not influenced by politics, and there is really perhaps the normal kind of appeal process that many feel that you could make.

And I guess the question for you, Mr. Twomey, and then I will let Mr. Feld comment on this. Do you feel the appeal mechanism is adequate enough for those people that have a problem with what ICANN is doing? And is there any way to make it a little bit easier to understand and what to do?

DR. TWOMEY. Good question, Chairman. And I think the answer is a two-part one.

One, I think that we do have, both through our ombudsman and then through the independent review process as we have the special board committee and then an independent panel of arbitrators, we do have an established system for review. Having said that, the board of ICANN is certainly conscious in its new principles, it is establishing, of its need to maintain very high standards of accountability.

So I think reviewing that is quite appropriate. And the board, I think, needs to be constantly looking at improving and always maintaining a high standard of accountability, and looking at those processes and see where they would work better.

MR. STEARNS. Have you had that many appeals?

DR. TWOMEY. We have had no party take an appeal to the final stage, the arbitrator, to conclusion.

MR. STEARNS. Now does that tell you anything, or is it just that you have been so impeccable in your credentials?

DR. TWOMEY. What it does tell you, Chairman, is that some of the parties have decided to go straight to the courts, and we haven't--quite separately, we defend quite a number of legal actions in courts.

MR. STEARNS. And do those overturn some of your decisions?

DR. TWOMEY. To date, no. There might be one potential interpretation of one decision about access to information by a board member, but apart from that particular decision, I don't think there has been a decision related to a contract that has been turned against ICANN--from my recollection.

MR. STEARNS. Mr. Feld, what do you think of the whole process of accountability for the decisions made by ICANN?

MR. FELD. Well, part of the problem is there are several levels of accountability, and the question of what is being looked at. Let me take the VeriSign renewal contract for dot com that we were just discussing. That was a contract that was negotiated between ICANN and VeriSign. Registrars, whose entire livelihood depends upon this, were not allowed to be privy to any part of that negotiation, were asked to comment upon

the entire package. And when seeking information on what was, for them, a critical element, this ability to raise prices, were unable to find any information, none has been forthcoming on where that has come from.

When I was in private practice, I used to do tariffing cases, and I can tell you for some clients that we had, the difference between a 10th of a cent on some things could be the difference between bankruptcy and profitability. So while not particularly of interest to end-users who are registering the names, it is a great deal of interest to at least one constituency. To be locked out of the critical part of that while it is being formulated, to be presented with an entire agreement afterwards and then to be told that the first step of a process for which there is no deadline while this is moving forward is to go to an employee of the people who just made the decision to try to work it out is not something that people whose livelihoods depend on this are going to find very attractive.

So I think that while I understand Dr. Twomey's perspective that there is a process that needs to be worked through, I would hope that there would be some understanding among the decision makers in ICANN of why so many people feel that critical aspects of the decision-making process are not subject to any kind of accountability check. When these things are reviewed by courts, they are not reviewed as an FTC action would be reviewed on. Was this decision arbitrary and capricious or in accordance with--in this case, we might say, the mandate of ICANN? They are reviewed under various theories of action, like antitrust, to try to somehow find a way to get the court to have jurisdiction over the issue. But if the court does not look to see that ICANN followed its processes, that is not what U.S. courts do.

MR. STEARNS. No, I understand. Is there anyone else that would like to comment on that particular question? Yes, Mr. Lenard?

MR. LENARD. Well, I think this just points up to the problem of ICANN taking on the functions of a regulatory agency. Obviously, one of the prime functions of the regulatory agency is setting--

MR. STEARNS. Couldn't the Department of Commerce step in here, though?

MR. LENARD. Well, I think whoever steps in it seems to me, the objective should not be to set up, quote, transparent or procedures, you know, that guarantee people due process. The objective should be to move away from that entire model and not have those, you know, regulatory functions, like I said in price ceilings, and to rely on competition, which Dr. Twomey says they are moving towards.

MR. STEARNS. So you would suggest a different regulatory model?

MR. LENARD. I would suggest moving away from monopoly-type regulatory model, which obviously price controls and price ceilings are a

prime element of, just not have price--not have those things at all, rely on competition to discipline the market. And the market is sufficiently competitive that that type of a regime is not justified even now.

MR. STEARNS. Yes, Mr. DelBianco.

MR. DELBIANCO. Yes. Earlier, I believe, Mr. Chairman, you asked a question about whether ICANN was sufficiently strong and independent to go on its own, this gets to that, this gets to the nub of it. If ICANN is perceived as having been too much under the control of one government, ours, other governments covet some piece of that power.

So I believe that in this transition to independence, that would abdicate us to do three things to demonstrate by our actions that we are serious about independence. The first is stop trying to interfere with decisions ICANN makes with private parties who negotiate contracts. Where contracts have to be sacrosanct, they have to be written in pen, and we all need to pay attention to process and transparency, but if somebody doesn't win a contract or doesn't like that their margins aren't going to be as big as they want, we can't let them believe they can simply run to Congress and change things.

Second quick thing is, let's avoid giving the U.N. any more excuses. Let's make sure we stay above the fray and don't interfere in any way with things like a .XXX, let's participate through the process.

And that was my third. We need to play the government advisory committee. We need to play very seriously there, go to the Internet Governance Forum and show that the U.S. is serious at being there on the Internet governance conversations, and being shoulder to shoulder with other nations on the process of Internet governance.

MR. BOHANNON. This discussion could get very abstract. I think there are actually two very specific things that I think we are frustrated with and I hope we have made it clear in our testimony. One is that ICANN made some commitments in the MOU in 2003 that they would take concrete steps to improve what is an existing policy for accuracy of "Whois" data. In our view, and it is reflected in the letter from 35 different organizations and different sectors, is that before the MOU that expires at the end of this month is renewed, we have got to have concrete obligations that are going to fulfill those requirements.

The second one, and I think it is a harder one, that we want to work with ICANN is that ICANN needs to make sure that the agreements they have with registrars are also enforced. Registrars have an obligation to collect accurate information. They are not doing it. The GAO found that more than 5 million domain name registrations in dot com and dot net are obviously false or misleading. That is not acceptable. And we need to work with ICANN so that we have a meaningful way to make sure that those kinds of agreements are enforced and that everyone's

obligations are met. So rather than talk about the broader ones, let's talk about what is really on the table now, what people have already agreed to do, and let's make sure that that gets done.

MR. STEARNS. Okay. If there is nothing else--Mr. Kneuer, anything you want to say? Okay. Mr. Twomey, I think you have got some marching orders, or at least you have heard some anyway. Let me just say, I think all of us on the committee think that ICANN is improving and is moving in the right direction, so that is good news and it has been educational for both the members and perhaps some of you, the witnesses here for our hearing. And I thank you for waiting through our votes. And with that the subcommittee is adjourned.

[Whereupon, at 4:55 p.m., the subcommittee was adjourned.]

RESPONSE FOR THE RECORD OF JOHN M. R. KNEUER, ACTING SECRETARY FOR COMMUNICATIONS AND INFORMATION, UNITED STATES DEPARTMENT OF COMMERCE

1. I'm concerned about the security and availability of the Internet, particularly of the dot com domain that carries trillions of dollars of American commerce every year. I know that we've experienced a number of denials of service and viruses attacks in the past and I assume that these are increasing. What is the magnitude of increase in the attacks, say, since 2000? Is it a five fold increase, a ten fold increase, what?

Answer: The Department remains committed to preserving the stability and security of the Internet domain name and addressing system (DNS). This commitment guides all of NTIA's activities in this area, including our recent Joint Project Agreement with ICANN. We continue to believe the private sector coordination of the technical management functions related to the DNS is the best approach to achieve stability and security given that the private sector has the tools and investment funds to rapidly react to new threats that are emerging daily. More specific information on specific incidents and attacks can be obtained from the United States Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). The US-CERT is charged with protecting the nation's Internet infrastructure by coordinating defense against and response to cyber attacks. The US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. The US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

2. Who is attacking the Internet? Are these just hackers doing this or is it something more? Is it organized crime, maybe international organized crime? Do we know if any of it is sponsored by foreign governments?

Answer: There are numerous classes of attackers on the Internet, including everything from state-sponsored efforts to home hobbyists. Preserving stability and security of the Internet DNS is a top priority of the Department. NTIA works very closely with a variety of U.S. government agencies, including the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS), Department of Defense Joint Task Force – Government Network Operations (JTF-GNO) and the National Cyber Security Division (NCSD) at DHS, to pursue appropriate national action and international collaboration across a range of legal, enforcement, administrative and technical areas to build a global culture of cybersecurity.

3. How do we protect ourselves and our economy from these attacks? ICANN is responsible for the domain name server registries, how do the registry companies - such as VeriSign, which is the registry for dot com - protect us against that increasing volume of attacks? Do they have to invest in additional infrastructure to increase their capacity? Do the registries have the resources they need to protect our resources?

Answer: Cybersecurity standards are developed by various industry organizations, such as the Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE), and adherence to the variety of standards is voluntary for the most part. While ICANN is not a standards organization, it does promote the adoption of industry standards through

its agreements with registry operators to comply with these standards. Registry agreements address the technical obligations, including compliance with the various industry developed standards, security requirements, and outage reporting that all registry operators must meet. In addition, each registry agreement contains a Service Level Agreement, which identifies the terms should the registry operator fall below the performance specifications. One standard that may help in this regard is the Domain Name System Security (DNSSEC) standard. NTIA has been actively working with an interagency working group to review the issues associated with the deployment of DNSSEC. Compliance with DNSSEC may require many of the providers of critical infrastructure to invest in additional infrastructure to increase their capacity.

4. If governance of the Internet were to move to an international body, such as the UN, or if the dot com registry were to go to a foreign company, what assurance do we, as Americans, have that our commerce and our economy will continue to be protected?

Answer: The Department of Commerce will continue to advocate for private sector leadership in the innovation and investment in the Internet while opposing calls for intergovernmental control. The success of the Internet is that it has been decentralized and private sector-led, encouraging individual creativity, access, and competition at all levels. The Department of Commerce is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the Internet DNS, including moving its governance to an international body such as the United Nations.

RESPONSE FOR THE RECORD OF DR. PAUL TWOMEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

Dr. Paul Twomey's responses to the follow-up questions from The Honorable C.L. "Butch" Otter

Relating to the September 21, 2006 Hearing of

Subcommittee on Telecommunications and the Internet, and

Subcommittee on Commerce, Trade, and Consumer Protection

Thank you again for the opportunity to appear before the Subcommittees, and thanks too for the follow-up questions you sent.

The first three questions all related to Internet security and specifically about details on Internet attacks. ICANN shares the Subcommittees' concerns about the security and stability of the Internet. Article I, section 1 of the ICANN Bylaws (copy attached) defines ICANN's mission as follows: "to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems." <http://www.icann.org/general/bylaws.htm>. ICANN's commitment to Internet security and stability is also demonstrated by the work of ICANN's Security and Stability Advisory Committee, comprised of noted industry technical experts <http://www.icann.org/committees/security/>.

ICANN is particularly concerned about the denial of service and other attacks referenced in the first follow-up question. Published data about the scale, magnitude, and targets of these attacks is incomplete due to several factors: public disclosure of an attack might reveal weaknesses in network infrastructure, attacks might target or result in the release of business proprietary or confidential information, the network operator might be embarrassed to disclose the attack, or might not even be aware that the attack took place. Still, it is clear that the size of any particular Distributed Denial of Service (DDoS) attack is becoming larger, due to the increasingly available bandwidth (broadband) that is available to the consumer, and the continued growth in the number of connected PCs in homes and businesses around the world. Services that are critical to ensuring the smooth operability of the Internet tend to "over-engineer" their networks, building them to handle load and bandwidth much higher than the service typically utilizes. This is done (at significant cost) to "soak" an attack, allowing the service to continue to operate during an attack while the organisation works with other network providers to push an attack back and away from the network(s) targeted. The Internet is made up of thousands of privately owned and operated, globally distributed networks working in conjunction with one another. Because of very nature of the Internet, "securing" it is best served through coordination of key engineers, corporate diligence, and embracing Best Common Practices (BCPs) published to help mitigate network threats.

Below are some links of interest that relate to Internet attacks or have additional relevant information:

http://www.us-cert.gov/

http://www.infragard.net/

http://www.internettrafficreport.com/

http://www.prolexic.com/zr/

http://www.cymru.com/monitoring/dnssumm/index.html

http://dnsmon.ripe.net/

Additional information about the nature and origins of attacks on the Internet could come from other domain-name service providers such as VeriSign and NeuStar that contract with both ICANN and the United States Government. ICANN carries out its coordination of the secure and stable operation of the domain-name system through a framework of contracts with private-sector operators of GTLDs such as .BIZ, .COM, and .ORG. Through these registry agreements, the GTLD operators are required to comply with Internet security and stability related standards and best practices. ICANN is in regular contact with, and receives regular reports from these and other DNS infrastructure providers concerning security and stability issues. ICANN ensures that the introduction of new registry services by GTLD operators is done in a stable and secure manner. ICANN has been assured in its role about the steps that the GTLD operators have taken to adequately safeguard these critical services, and ICANN continues to be impressed by the operators' exemplary performance history. The Subcommittees might want to ask these companies and others directly for additional relevant information.

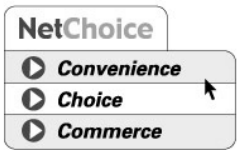
The fourth follow-up question dealt with Internet governance and the world economy. The use of the term 'governance' is broad, and is generally understood to cover a wide range of governance related questions that affect the different layers and use of the Internet -- ranging from the coordination of the Internet's unique identifier system to the content and uses by users of the Internet (i.e. the layers above the underlying infrastructure).

Broadly stated, the Internet's successful development is due to the engagement of among others, the private sector, technical community, users, and governments in both its development and decision-making surrounding its use. This multi-stakeholder approach has resulted in the Internet's evolution globally in ways unanticipated and which have benefited America's commerce and economy.

The Internet's continued development, that benefit the American commerce and economy must continue to see a "governance" mechanism that involves all stakeholders, and is private sector driven. As the Internet continues to evolve, and its users expand globally, this multi-stakeholder approach evolves as well. Decisions affecting different issues arising from the Internet (whether the unique identifier system, or other areas) have been effective when taken from a multi-stakeholder, consensus driven approach. That is, the mechanism by which governance has been achieved to date, through an international multi-stakeholder approach, has a demonstrated success in addressing issues requiring attention rapidly while not stifling innovation or development. An inter-governmental approach would not achieve this.

Thank you for your attention. Please do not hesitate to contact me or my staff if I can be of any further assistance.

RESPONSE FOR THE RECORD OF STEVE DELBIANCO, VICE PRESIDENT FOR PUBLIC POLICY, ASSOCIATION FOR COMPETITION TECHNOLOGY, ON BEHALF OF NETCHOICE COALITION



Promoting Convenience, Choice, and Commerce on The Net

The NetChoice Coalition
1401 K St NW, Suite 502
Washington, DC 20005
www.netchoice.org

November 1, 2006

ICANN Internet Governance: Is It Working?
Hearing Date: September 21, 2006
Subcommittee on Telecommunications and the Internet and Subcommittee on Commerce, Trade, and Consumer Protection

Answers to follow-up questions by The Honorable C.L. "Butch" Otter
Prepared by Steve DelBianco
Executive Director, NetChoice

Question 1: What is the magnitude of the increase in the attacks, say, since 2000?

The many communications devices that make our lives more efficient and allow us to communicate faster are unfortunately also vulnerable targets for expanded Internet attacks. According to CipherTrust, computer hackers hijack more than 180,000 computers each day so that they can steal computing power to perpetrate attacks on larger networks. These attacks have grown by almost seven-fold in the past year, according to Symantec.

The same forces that are helping our economy to expand are also allowing extortion rackets to expand their reach to victimize far less sophisticated Internet users

The security of the Internet's core infrastructure is a key component for keeping the Internet user safe. Given the increased number of attacks the companies who are responsible for the core infrastructure must continually strengthen their firewalls and secure all transactions to ensure consistent, fast, efficient response times for an Internet that is "always on" and available to a worldwide user base.

The companies who are responsible for these Infrastructure build outs need to have a forward operating plan that scales at least ten times the level of volume they expect the network to expand each year if not larger. The key to keeping ahead of the usage curve is the ability and incentive to invest heavily in system infrastructure.

A powerful incentive for registry operators to keep investing in infrastructure is the expectation that their contracts will be renewed if they've met performance requirements and honored all terms of their contract.

As I said in testimony before the House Small Business Committee in June, I have some first-hand experience with service contracts, since my own business was selected to provide software help-desk support for a large credit card company. I invested heavily in hiring and training help-desk staff, rented new space for the operation, acquired new computers and integrated a call management system. We even bought electronic scrolling sign boards to alert the staff about callers in the queue and hold times.

To have any hope of recovering this huge up-front investment, I insisted on renewal terms that gave us a favorable chance to renew the contract after its initial term. To earn

the renewal, we had to satisfy several metrics for service levels. In addition, we could not have any sustained failures to meet new or emergency initiatives that could be expected over the term of the contract. "Best efforts" wouldn't be good enough—we had to be able to recover and deliver if unexpected call volumes hit us out of the blue.

My experience is fairly typical, and tells me that ICANN is right to include a renewal option in its registry contracts. While a renewal option helps the incumbent to retain the contract upon expiration, the incumbent will lose the contract if it fails to satisfy the functional requirements in the new contract.

Question 2: Who is attacking the Internet? Are these just hackers doing this or is it something more? Is it organized crime, maybe international organized crime? Do we know if any of it is sponsored by foreign governments?

We don't know exactly who is attacking the Internet, but the emerging attack profile suggests ways to mitigate the activity once it's identified by a network operator. I understand that several government agencies are aware of this activity and work with Internet infrastructure companies to fight organized attackers. Speculation is that some attackers are organized efforts by crime factions, intended to show their computing firepower and their ability to disrupt networks.

I have no specific information regarding state-sponsored attacks. However, I think that several states are far too tolerant of criminal activity coming from within their borders. Brazil, Poland, Romania, Romania, and Russia, for instance, host underground economies built upon counterfeit goods. These nations tolerate high rates of computer software piracy, make millions of counterfeit DVDs, and produce, deal, or traffic in fake consumer merchandise. To the extent they are hospitable to counterfeiting rings, these nations are also likely to be hosting organized Internet attack groups.

Question 3: How do we protect ourselves and our economy from these attacks? How do registry companies—such as VeriSign, the registry for dot com—protect us against the increasing volume of attacks? Do they have to invest in additional infrastructure to increase their capacity? Do the registries have the resources they need to protect our resources?

The best way to protect yourself as an individual user is to keep your anti-virus software and operating system up to date. The next step is to educate your family and employees on situational awareness tactics so they identify threats from phishing or spyware. Denial of service attacks are often extended versions of what seem like simple abuses to an individual user.

Registries, on the other hand, employ a range of measures to thwart attacks on the domain name system:

> **Over-provisioning**. Registry operators invest in extra capacity, or "over-provisioning" in order to handle much higher transaction volumes, such as those that occur during denial of service attacks.
>
> **Redundant Systems**. Registries invest in multiple, parallel systems to provide redundancy in the event that main systems are disabled.
>
> **Geographical Distribution.** Backup servers and facilities are hosted in geographically diverse locations to mitigate risks of physical disasters and of attacks on routers serving any single area of DNS servers.
>
> **Disaster Recovery.** Registry operators prepare detailed plans and practices to enable a quick recovery from attacks and other disasters.
>
> **Personal Vigilance**. The largest registry operators can afford to hire experienced security professionals to manage all of these security systems investments, 24x7x365.
>
> **International Cooperation**. The larger registry operators are in constant communications and coordination with law enforcement and industry allies across the globe.

Registries have access to the technology tools they need, but ICANN needs to maintain contractual incentives so that registry operators will continue to invest in security systems throughout the term of their contracts.

Question 4: If governance of the Internet were to move to an international body, such as the UN, or if the dot com registry were to go to a foreign company, what assurance do we, as Americans, have that our commerce and our economy will continue to be protected?

For the private sector to continue its success in managing and developing the Internet, one element is absolutely critical: *continued reliance on the clarity and certainty of contracts*.

Operators of Internet infrastructure rely upon contracts with ICANN that clearly describe responsibilities and restrictions. As contract participants, these operators make significant investments in people, equipment, and long-term network contracts in order to secure the Internet. These contracts must therefore be honored by ICANN, without risk of being unilaterally abrogated or modified in response to a change of sentiments among ICANN participants.

Moreover, these contracts must be upheld and interpreted by a reliable and consistent body of law. For the present, U.S. Courts serve as the place to govern contract disputes between operators and ICANN. If an international governance body were to take over ICANN's role as contract partner for Internet operations, the clarity and certainty of these infrastructure contracts would be thrown into doubt.

Even if ICANN offices or the distributive root server were to move out of the U.S., I believe that U.S. Courts should still be the way to resolve disputes arising out of ICANN contracts.

RESPONSE FOR THE RECORD OF THOMAS M. LENARD, SENIOR VICE PRESIDENT FOR RESEARCH, THE PROGRESS & FREEDOM FOUNDATION

"ICANN Internet Governance: Is It Working?"
September 21, 2006 hearing
Responses to questions from The Honorable C.L. "Butch" Otter
For Thomas M. Lenard

Answer to Question 1:

I don't have a precise answer to the question, but the following figures indicate that it is a large and growing problem. According to security company CipherTrust, more than 180,000 PCs are turned into zombies every day. Symantec estimates that there has been a 700-percent increase in bot-nets over the past year.

Answer to Question 2:

There seems to be evidence that well-funded organized crime groups, increasingly located in other countries, use networks of bots to obtain financial information.

Answer to Question 3:

Protection will come from having a well-functioning private sector that has the right incentives to invest in security. This is why my testimony recommends moving away from a regulatory model for registries. These companies need to have the right incentives to invest in the additional infrastructure that will increase security and the regulatory model may interfere with those incentives.

Answer to Question 4:

I would be concerned that, despite the problems we have had with ICANN, an international body would be more regulatory. This would interfere with incentives to invest in capacity and security, which would have an adverse effect on the Internet, e-commerce and the economy in general.

RESPONSE FOR THE RECORD OF HAROLD FELD, SENIOR VICE PRESIDENT, MEDIA ACCESS PROJECT

Mr. Fred Upton
Chairman
Subcommitee on Telecommunications
and the Internet
U.S. House of Representatives
Committee on Energy and Commerce

Mr. Cliff Stearns
Chairman
Subcommittee on Commerce, Trade
and Consumer Protection
U.S. House of Representatives
Committee on Energy and Commerce

November 27, 2006

Dear Mr. Upton and Mr. Stearns:

Thank you for forwarding to me the additional questions from Mr. Otter with regard to the joint hearing by your Subcommittees on September 21, 2006 entitled "ICANN Internet Governance: Is It Working?"

Unfortunately, the questions provided fall outside of my area of expertise, and outside the expertise of the Media Access Project generally. I regret that I can provide no useful information to the Subcommittees in response.

If there is any other way I can be of further assistance in this matter, please feel free to contact me at (202) 454-5684, or hfeld@mediaaccess.org.

Sincerely,

Harold Feld
Senior Vice President

RESPONSE FOR THE RECORD OF MARK BOHANNON, GENERAL COUNSEL AND SENIOR VICE PRESIDENT, PUBLIC POLICY, SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

Questions for Mark Bohannon
General Counsel & SVP Public Policy
Software & Information Industry Association (SIIA)

From

Hon. C.L. "Butch" Otter

1. I'm concerned about the security and availability of the Internet, particularly of the dot com domain that carries trillions of dollars of American commerce every year. I know that we've experienced a number of denials of service and viruses attacks in the past and I assume that these are increasing. What is the magnitude of the increase in the attacks, say, since 2000? Is it a five fold increase, a ten fold increase, what?

SIIA member companies, leaders in software, digital content, eBusiness and Internet products and services, experience denial of service attacks, unauthorized intrusions and network and application viruses. SIIA does not collect independent statistics on these incidences.

Among experts, there is a well-documented challenge in having a common basis for measuring and evaluating such attacks. As one report from the CERT indicated:

> "In the cyber world, the current state of the practice regarding the technical ability to track and trace Internet-based attacks is primitive at best. Sophisticated attacks can be almost impossible to trace to their true source using current practices. The anonymity enjoyed by today's cyberattackers poses a grave threat to the global information society, the progress of an information based international economy, and the advancement of global collaboration and cooperation in all areas of human endeavor."[1]

Symantec, a member of SIIA, has published a regular semi-annual "Symantec Internet Security Threat Report" that has tracked the latest attacks and trends in Internet security since 2002. While the Report focuses on more than traditional denial of service attacks, the numbers are a useful reference point. In its latest report, published September 2006, Symantec:

> " … documented 2,249 new vulnerabilities in the first half of 2006. This is an increase of 18% over the 1,912 vulnerabilities that were documented in the second half of 2005. It is also a 20% increase over the 1,874 vulnerabilities that were reported in the first half of 2005. Symantec documented a higher volume of

[1] Howard F. Lipson, Ph.D., CERT® Coordination Center, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", November 2002, found at: http://www.cert.org/archive/pdf/02sr009.pdf

> vulnerabilities in this reporting period than in any other previous six-month period.

> "The marked increase in the number of vulnerabilities can be attributed to the continued growth in those that affect Web applications. Web applications are technologies that rely on a Web browser for their user interface, rely on HTTP as the transport protocol, and reside on Web servers. Microsoft Internet Explorer was the most frequently targeted Web browser, accounting for 47% of all Web browser attacks. Vulnerabilities affecting Web applications accounted for 69% of all vulnerabilities that were documented by Symantec in the first half of 2006. This is a slight increase over the 68% disclosed in the second half of 2005. It is also a nine percentage point increase over the 60% documented in the first half of 2005. The high number of these vulnerabilities is due in part to the popularity of Web applications and to the relative ease of discovering vulnerabilities in Web applications compared to other platforms. Web applications are required to accept and interpret input from many different sources, and there are very few restrictions to distinguish valid input from invalid. This is further complicated because Web browsers, the application through which most Web applications operate, are very liberal in what they will accept and interpret as valid input."[2]

More specifically, "[o]ver the last six months of 2005, Symantec detected an average of 1,402 DoS attacks per day (figure 3). This is an increase of 51% from the first half of 2005, when Symantec detected an average of 927 DoS attacks per day."[3] For the first half of 2006, Symantec "observed an average of 6,110 DoS attacks per day."[4]

"Symantec Internet Security Threat Report: Trends for January 06–June 06," Volume X, Published September 2006, pg. 6. Found at: http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.

[3] "Symantec Internet Security Threat Report: Trends for July 05-December 05", Volume IX, Published March 2006, pg. 12. Found at: http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf.

[4] Volume X, pg. 16.

2. Who is attacking the Internet? Are these just hackers doing this or is it something more? Is it organized crime, maybe international organized crime? Do we know if any of it is sponsored by foreign governments?

According to one study conducted, the top twenty geographical sources of Internet attacks

included:

Geographical distribution of Internet attacks and probes

Rank	% of total	Country
1	27.38	China
2	21.16	USA
3	6.03	South Korea
4	2.82	Canada
5	2.04	Hong Kong
6	2.00	Russia
7	1.88	Spain
8	1.77	the Philippines
9	1.72	Japan
10	1.63	Taiwan
11	1.25	Germany
12	1.25	the Netherlands
13	1.13	United Kingdom
14	0.72	France
15	0.41	Italy
16	0.39	Brazil
17	0.31	Switzerland
18	0.29	India
19	0.25	Poland
20	0.22	Uruguay

Geographical distribution of Internet attacks and probes

Source: Costin Raiu, Head of Research & Development, Kaspersky Lab Romania, "Internet Attacks 2005", published Feb. 17, 2006. Found at: **http://www.viruslist.com/en/analysis?pubid=180265451#geo**.

While we are aware of anecdotal information about whether these attacks originate with governments (See, e.g., White House Confirms Denial Of Service Attack - Government Activity, Newsbytes News Network, May 23, 2001 at: **http://www.findarticles.com/p/articles/mi_m0NEW/is_2001_May_23/ai_74988164**), we do not have information available to us that can quantify this level.

I am also enclosing a set of PowerPoint documents that confirm the trends in the above report. These focus on the *targets* of attacks, as well as sources (using another methodology). These are from the September 2006 Symantec Report previously referred to.

3. How do we protect ourselves and our economy from these attacks? ICANN is responsible for the domain name server registries, how do the registry companies -- such as VeriSign, which is the registry for dot com – protect us against the increasing volume of attacks? Do they have to invest in additional infrastructure to increase their capacity? Do the registries have the resources they need to protect our resources?

To protect ourselves and our economy requires an on-going effort by government, industry, academic and citizens to assess the vulnerabilities and threats we face, and identify appropriate initiatives to combat them and enhance our security. In many respects, The National Strategy to Secure Cyberspace outlined many of the steps that are required. (See http://www.whitehouse.gov/pcipb/executive_summary.pdf.)

In this context, the role of ICANN is a limited one focused on the technical management of the Domain Name System. We note that ICANN established DNS Root Server System Advisory Committee shortly after its formation. It's work can be tracked at: http://www.icann.org/committees/dns-root/.

4. If governance of the Internet were to move to an international body, such as the UN, or if the dot com registry where to go to a foreign company, what assurance do we, as Americans, have that our commerce and our economy will continue to be protected?

As the discussion at the hearing indicated, there was little support for moving the functions of ICANN to an international body, such as the UN. Even if such a move were to occur, there was little basis for suggesting that moving the "A" root server out of the U.S. was warranted in the foreseeable future.

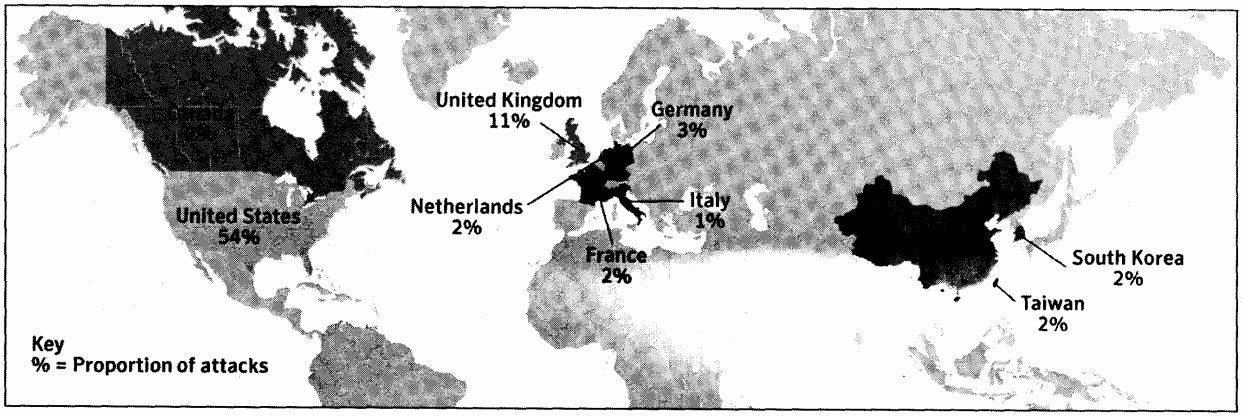
Attack Trends – Denial of Service - Top Targeted Sectors

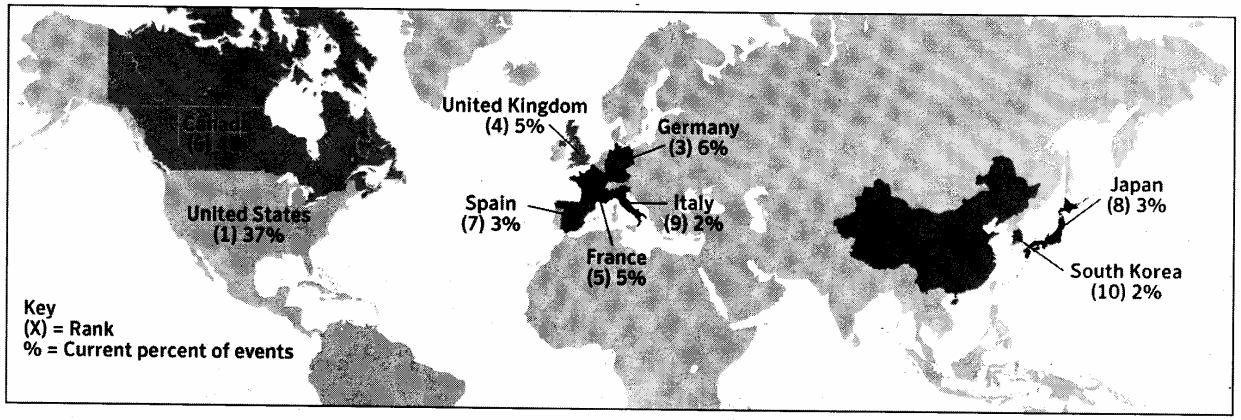
- Internet Service Providers - bigger net = more fish
- Government - high profile
- Telecom - regional, smaller ISP's.

Rank	Sector	Proportion of attacks
1	Internet Service Provider	38%
2	Government	32%
3	Telecommunications	8%
4	Transportation	4%
5	Education	3%
6	Accounting	3%
7	Utilities / Energy	3%
8	Insurance	3%
9	Financial Services	2%
10	Information Technology	2%

Attack Trends – Denial of Service - Top Target Countries

- Average of 6,110 Denial of Service attacks per day
- Average 4,000 daily in January to 7,500+ per day in June
  - One period in March saw a spike to 8,000+
- The U.S. was the most targeted nation for DoS attacks followed by China and the United Kingdom



Attack Trends – Top Originating Countries

- The United States remains the top source country for attacks with 37% of the worldwide total. Attacks originating from the United States grew by 29% due to a large increase in broadband users.
- China increased from 7% to 10% of the worldwide total. Attacks grew by 37%.
- The United States (40%) and China (20%) were the main source of attacks detected by sensors in the Financial Services industry. Attacks originating in China increase by 90% over the previous reporting period.