

Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(*pro hac vice application pending*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORP., FS-ISAC, INC., and
NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO,
Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX,
Harderman, Gribodemon, Aqua, aquaSecond, it,
percent, cp01, hct, xman, Pepsi, miami, miamibc,
petr0vich, Mr. ICQ, Tank, tankist, Kusunagi,
Noname, Lucky, Bashorg, Indep, Mask, Enx,
Benny, Bentley, Denis Lubimov, MaDaGaSka,
Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel
Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D
frank, duo, Admin2010, h4x0rdz, Donsft,
mary.J555, susanneon, kainehabe, virus_e_2003,
spaishp, sere.bro, muddem, mechan1zm,
vlad.dimitrov, jheto2002, sector.exploits AND
JabberZeus Crew CONTROLLING COMPUTER
BOTNETS THEREBY INJURING PLAINTIFFS,
AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

FILED UNDER SEAL

U.S. DISTRICT COURT
EASTERN DISTRICT
OF NEW YORK

2012 MAR 19 AM 9:52

FILED
CLERK

CV 12-1335

MANN. M.J.

**DECLARATION OF JACOB M. HEATH IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER,
SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Jacob M. Heath, declare as follows:

1. I am an attorney with the law firm of Orrick, Herrington & Sutcliffe LLP (“Orrick”), counsel of record for Plaintiff Microsoft Corp. (“Microsoft”). I make this declaration in support of Plaintiffs’ Application For An Emergency Temporary Restraining Order, Seizure Order And Order To Show Cause Re Preliminary Injunction (“Application”). I make this declaration of my own personal knowledge and, if called as a witness, I could and would testify competently to the truth of the matters set forth herein.

I. PARTIES

2. Plaintiffs seek an *Ex Parte* Temporary Restraining Order, Seizure Order And Order To Show Cause Re Preliminary Injunction to disable the Internet domains and the IP addresses and to seize the command and control servers and software used by the John Doe Defendants (“Defendants”) to operate the Zeus Botnets. A “botnet” is a network consisting of end-user computers connected to the Internet that have been infected with a certain type of malicious software that places the infected end-user computer under the control of the individuals and organizations operating the botnet. Those individuals and organizations utilize the infected end-user computers to conduct illegal activity.

3. As counsel of record for Plaintiff Microsoft, I have participated in Microsoft’s previous efforts to disable other computer botnets including the “Waledac” Botnet in February 2010, the “Rustock” Botnet in March 2011, and the “Kelihos” Botnet in September, 2011. Based on my previous experience with similar botnet-defendants, *ex parte* relief is necessary, as notice to Defendants would allow them to destroy the evidence of their illicit activity and give them an opportunity to move the instrumentalities they used to conduct their unlawful activity, rendering the further prosecution of this matter futile. Based on my prior experience, I am aware that in one previous effort to disable the Rustock Botnet, the operators of the Rustock Botnet – after learning of the attempt to disable the botnet – managed to migrate that botnet’s command and control infrastructure to new IP addresses. The Rustock-infected end-user computers were then directed to new IP addresses.

4. Plaintiffs’ counsel has not attempted to provide notice of the Application, and

notice should not be required to provide notice at this time. I respectfully submit that good and sufficient reasons exist for this Application to be made by Order to Show Cause in lieu of by notice of motion. Plaintiffs have not sought previously this particular *ex parte* relief in the United States District Court for the Eastern District of New York as to these Defendants.

5. Certain Internet domains have been identified as part of the command and control infrastructure of the Zeus Botnets. The Internet domains names and their respective domain registries are set forth at Appendix A to the Complaint.

6. Certain IP addresses have been identified as part of the command and control infrastructure of the Zeus Botnets. The IP addresses and their respective hosting companies are set forth at Appendix B to the Complaint.

7. Certain specific internet file paths have been identified as part of the command and control infrastructure of the Zeus Botnets. The file path and contact information for the respective free web posting services are set forth at Appendix C to the Complaint.

8. I have conducted research in an effort to identify the Defendants associated with these domains and IP addresses. I have been unable to determine the true identities of Defendants. Based on my prior experience and based on my research regarding these domains and IP addresses, it is likely that the contact information for the individuals or entities that operate the Internet domains and IP addresses have been provided by Defendants to these Internet domain name registries and web hosting companies, through the domain name and IP address registration process. This information may include individual and entity names, physical addresses, email addresses, facsimile numbers and telephone numbers. I have reviewed the requirements to sign up for services and the terms of service relating to the Internet domains and IP addresses and conclude, based on this research, that such contact information is likely to be in the possession of these companies.

9. To the extent that such information has been provided by Defendants, the information most likely to be accurate are e-mail addresses as, upon information and belief,

such are necessary to register for Internet domains or IP address hosting services. It is more likely that the email addresses exist and are functional than it is likely that the personal names and physical addresses are correct or accurate. I conclude this in part based on the fact that when domain registrants set up Internet domains they must receive confirmation from the domain registrar via email in order to utilize and access the domains. Other contact information, such as physical address information, is more likely to be false. I base this conclusion, in part, on past experiences relating to botnets in which registration name, address and telephone number were determined to be fraudulent, but the email address provided by defendants was, in fact, associated with them. Further supporting this conclusion, in May 2010, the Internet Corporation for Assigned Names and Numbers (“ICANN”) – an organization that administers the domain name system – issued a study indicating the ease with which name and physical mailing addresses for domain registrations may be falsified. Attached hereto as Exhibit 1 is a true and correct copy of the ICANN’s May 2010 study, “WHOIS Proxy/Privacy Service Abuse – Definition.”

10. Based on my prior experience and from my research, I believe that the most reliable contact information for effecting communication with Defendants are email addresses and messaging addresses that have been discovered to be associated with defendants and the contact information, particularly email addresses, in possession of the domain registries and web hosting companies. From my research, I conclude that such contact information is likely to be valid, as it is necessary to obtain Internet domain name or web hosting services. Upon provision of such contact information by the Internet domain registries and web hosting companies to Plaintiffs, notice of this proceeding and service of process may be attempted using such contact information. Through my research, I have not discovered any other information that would enable, at this point, further identification of or contact with Defendants other than that in the possession of these companies. I believe that absent an order directing Doe discovery, these companies will be unlikely to share contact information necessary to provide notice and service to Defendants.

II. NOTICE AND SERVICE OF PROCESS

A. Plaintiffs Have Robust Plans To Provide Notice

11. On behalf of Plaintiffs, Orrick will attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint by sending the pleadings and/or links to the pleadings to e-mail addresses, messaging addresses, facsimile numbers and mailing addresses associated with Defendants or otherwise provided by Defendants to the Internet domain registries and IP address hosting companies.

12. On behalf of Plaintiffs, Orrick will attempt notice of any TRO, preliminary injunction hearing and service of the complaint by publishing those pleadings on a publicly accessible website located at: <http://www.zeuslegalnotice.com/>. Orrick will publish such notice on the website for a period of six months. The following information will be made available on the website:

- a. The information contained in the case caption and the content of the summons.
- b. The following summary statement of the object of the complaint and the demand for relief: "Plaintiffs Microsoft Corporation ("Microsoft"), National Automated Clearing House Association ("NACHA") and Financial Services – Information Sharing and Analysis Center ("FS-ISAC") have sued defendants John Does 1-39 associated with the Internet Domains and Internet IP Addresses listed below. Plaintiffs allege that Defendants have violated Federal and state law by operating a computer botnet through these Internet domains and Internet IP addresses, causing unlawful intrusion, intellectual property violations and dissemination of unsolicited bulk email to the injury of Microsoft and the public. Plaintiffs seek a preliminary injunction and seizure order directing the registries and web hosting companies associated with these Internet domains and IP addresses to take all steps necessary to disable access to and operation of these Internet domains and IP addresses, ensure that changes or access to the Internet domains and IP addresses cannot

be made absent a court order and that all content and material associated with these Internet domains and IP addresses is to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at <http://www.zeuslegalnotice.com/>.”

- c. The date of first publication.
- d. The following text: “NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must “appear” in this case or the other side will win automatically. To “appear” you must file with the court a legal document called a “motion” or “answer.” The “motion” or “answer” must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the Plaintiffs’ attorneys, Richard A. Jacobsen at Orrick, Herrington & Sutcliffe, LLP, 51 West 52nd Street, New York, New York 10019 or Gabriel M. Ramsey at Orrick, Herrington & Sutcliffe LLP, 1000 Marsh Rd., Menlo Park, California, 94025. If you have questions, you should consult with your own attorney immediately.”

13. On behalf of Plaintiffs, Orrick will attempt notice of any TRO, preliminary injunction hearing and service of the complaint by publishing the above notice language and a link to <http://www.zeuslegalnotice.com/> in the local language in general circulation newspapers in Russia, Ukraine and Romania, where Defendants are generally believed to reside.

14. On behalf of Plaintiffs, Orrick will serve each of the Internet domain registries listed at Appendix A to the Complaint, the web hosting companies listed at Appendix B to the Complaint and the free website hosting services at Appendix C to the Complaint with copies of all documents served on Defendants.

15. On behalf of Plaintiffs, Orrick will retain a national service of process firm to

attempt notice of any TRO and preliminary injunction hearing, as well as service of the complaint by personal delivery on any Defendant in this case that has provided contact information in the United States. Upon execution of any TRO, Orrick will instruct the process server to deliver these documents to any U.S. addresses associated with Defendants.

16. On behalf of Plaintiffs, Orrick will prepare Requests for Service Abroad of Judicial or Extrajudicial Documents to attempt notice of any TRO and preliminary injunction hearing, as well as service of the Complaint on any Defendants in this case that have provided contact information in foreign countries that are signatories to the Hague Convention on Service Abroad or any similar treaty, and will comply with the requirements of those treaties. Upon entry of any TRO, Orrick will execute and deliver these documents to the appropriate Central Authority and request, pursuant to the Hague Convention or similar treaty, that the Central Authority deliver these documents to the contact information provided by Defendants. I am informed, and therefore believe, that notice of the preliminary injunction hearing and service of the Complaint could take approximately three to six months or longer through this process.

17. Plaintiffs have not and will not publicize the requested seizure until after the requested seizure is carried out.

B. Notice Under ICANN Domain Name Registration Policies

18. Attached hereto as Exhibit 2 is a true and correct copy of a document describing ICANN's role. Exhibit 2 reflects the following. ICANN is a not-for-profit partnership formed in 1998. ICANN coordinates domain names and IP addresses (unique identifying numbers for computers throughout the world), which enables the operation of the global Internet. ICANN's responsibilities include running an accreditation system for domain name "registrars." Domain name registrars enter into arrangements with individual "registrants" who wish to register particular domain names. ICANN has a contractual relationship with all accredited registrars that set forth the registrars' obligations. The purpose of the requirements of ICANN's accreditation agreements with registrars is to

provide a consistent and stable environment for the domain name system, and hence the Internet.

19. A true and correct copy of the accreditation agreement between ICANN and domain name registrars in use before May 21, 2009 is attached hereto as **Exhibit 3**.

20. A true and correct copy of the accreditation agreement between ICANN and domain name registrars in use on or after May 21, 2009 is attached hereto as **Exhibit 4**.

21. The following summarizes provisions set forth in the ICANN accreditation agreements with registrars at Exhibits 3 and 4.

1. **ICANN Requires That Registrants Agree To Provide Accurate Contact Information**

22. Section 3.7.7.1 of the accreditation agreement provides that domain registrants will provide the registrar accurate and reliable contact information. In particular, the domain name registrant:

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

23. Section 3.7.7.2 of the accreditation agreement provides that if the registrant fails to respond for over 15 days to a registrar’s inquiry about inaccurate contact information, the domain may be cancelled. In particular, the domain name registrant’s:

“willful provision of inaccurate or unreliable information, its willful failure to promptly update information provided to Registrar, or its failure to respond for over fifteen (15) calendar days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder’s registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for cancellation of the Registered Name registration.”

2. ICANN Requires That Registrants Agree To A Dispute Resolution Policy Under Which Notice Is Given By Sending The Complaint To The Registrant's Contact Information

24. Section 3.8 of the accreditation agreement provides that registrars shall require registrants to agree to the Uniform Domain Name Dispute Resolution Policy ("UDRP"). The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars. Attached hereto as **Exhibit 5** is a true and correct copy of the UDRP.

25. As part of the registrant's agreement to the UDRP, the registrant agrees to the Rules for Uniform Domain Name Dispute Resolution Policy ("Rules"). Attached hereto as **Exhibit 6** is a true and correct copy of the Rules.

26. Pursuant to the Rules, "Written Notice" of a complaint regarding a domain requires electronic transmittal of the complaint to a domain registrant and hardcopy notification that the complaint was sent by electronic means. In particular, "Written Notice" is defined as:

"hardcopy notification by the Provider to the Respondent of the commencement of an administrative proceeding under the Policy which shall inform the respondent that a complaint has been filed against it, and which shall state that the Provider has electronically transmitted the complaint including any annexes to the Respondent by the means specified herein. Written notice does not include a hardcopy of the complaint itself or any annexes."

27. Pursuant to the Rules, notice of a complaint may be achieved by the registrar forwarding the complaint to the postal address, facsimile number and e-mail addresses of the domain registrant. In particular, the Rules define the procedure for providing notice as follows:

"(a) When forwarding a complaint, including any annexes, electronically to the Respondent, it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility:

(i) sending Written Notice of the complaint to all postal-mail and facsimile addresses (A) shown in the domain name's registration data in Registrar's Whois database for the registered domain-name holder, the technical contact, and the administrative contact and (B) supplied by Registrar to the Provider for the registration's billing contact; and

(ii) sending the complaint, including any annexes, in electronic form by e-mail to:

(A) the e-mail addresses for those technical, administrative and billing contacts;

(B) postmaster@<the contested domain name>; and

(C) if the domain name (or “www.” followed by the domain name) resolves to an active web page other than a generic page the Provider concludes is maintained by a registrar or ISP for parking domain-names registered by multiple domain-name holders), any e-mail address shown or e-mail links on that web page; and

(iii) sending the complaint, including any annexes, to any e-mail address the Respondent has notified the Provider it prefers and, to the extent practicable, to all other e-mail addresses provided to the Provider by Complainant...”

28. The effect of the UDRP and the Rules is that domain name registrants agree that notice of a complaint relating to their domains may be provided by the foregoing means, including by sending the complaint to postal, facsimile and email addresses provided by registrants.

3. **ICANN Requires That Registrants Agree That Domains May Be Suspended Or Cancelled Pursuant To The Dispute Resolution Policy**

29. Section 3.7.7.11 of the accreditation agreement provides that registrars shall require that a domain name registrant “shall agree that its registration of the Registered Name shall be subject to suspension, cancellation or transfer” pursuant to ICANN’s policies for the resolution of disputes concerning domain names.

4. **ICANN Requires That Registrants Agree Not To Use Domains In An Illegal Manner**

30. Under Section 2 of the UDRP, the domain registrant agrees that:

“By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to

determine whether your domain name registration infringes or violates someone else's rights."

31. Similarly, section 3.7.7.9 of the accreditation agreement provides that the domain name registrant "shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party."

C. **Notice Under Web Hosting Companies Terms, Conditions, Policies, And Service Agreements**

1. **Web Hosting Companies Send Account-Related Information To Customer-Provided Contact**

32. The terms of service of the Internet domain registrars and web-hosting companies provide for sending account-related notices to contact information provided by the customers, including, on information and belief, Defendants. For example, the terms of service for **Network Operations Center, Inc./BurstNET, Inc.** provide, for example, that:

"Client agrees to provide BurstNET® with accurate, complete and updated information required by the registration/initiation of the BurstNet® service (Client Registration Data), including Client's legal name, address, telephone number(s), and applicable payment data (e.g., credit card number and expiration date). Client agrees to notify BurstNET® within thirty (30) days of any change in Client Registration Data. Failure to comply fully with this provision may result in immediate suspension or termination of your right to use BurstNET® Services."

33. A true and correct copy of the terms and service of Network Operation, Inc./BurstNET is attached hereto as **Exhibit 7**. Based on my pasted experience and on information and belief, the other web hosting services used by Defendants require that similar contact information be provided.

2. **Web Hosting Terms Of Service Prohibit Customers From Using Services In An Illegal Manner**

34. The Internet domain registrars and web hosting terms of service prohibit customers, including, on information and belief, Defendants, from use the services in an illegal manner, and customer accounts may be terminated for violation of those terms. The

terms of service for Network Operations Center, Inc./ BurstNET, Inc. provide, for example, that:

- “Copyright and Proprietary Materials. You should be aware that much of the Content available on the Internet is protected by copyright, trademarks, trade secrets and other rights of the independent third parties or their licensors who make such content available on the Internet. Clients use of such Content will be subject to the specific restrictions place on such Content by the owners or licensors of the Rights in such Content and all applicable laws and regulations. Transmitting to the Internet or posting on your site copyright or other material of any kind which is subject to rights of any person or entity without the express permission of the right's holder is prohibited and will result in termination of your BurstNET® Service and possible civil and /or criminal liability.” (Terms of Service, Exhibit B, ¶7).
- “Your use of the Internet is subject to all applicable local, state, national, and international laws and regulations, Without limiting the other rights available to BurstNET®, BurstNET® retains the right but not the obligation, in its sole discretion and without prior notice or liability, to restrict and/or terminate your access to the Internet and BurstNET® services, if your use of the Internet violates any such laws or regulations, any prohibitions upon your conduct in connection with the Internet raised in this paragraph or otherwise restricts or inhibits any other user from enjoying the Internet or their BurstNET® services.” (Terms of Service, Exhibit B.)
- “Illegal Usage Restrictions: Resources provided by BurstNET® may be used only for lawful purposes. Examples of unlawful content include, but are not limited to:
 - unlicensed hosting of, linking to, or any involvement in the transmission of copyrighted media, applications, published works, or any data protected by trade secret, without sufficient [...]
 - fraudulent sites and other forms of “phishing” (emails/forms/sites used to gather personal information from unsuspecting individuals) [...]” (Terms of Service, Exhibit D)
- “Prohibited Usage Restrictions: In addition to activities governed by law, BurstNET® strictly prohibits: [...]
 - malware (malicious software) and/or botnets [...]
 - mail bombing, email address harvesting, and/or unsolicited email (including bulk mail sent to unconfirmed recipients and individual unsolicited advertisement or link exchange [...])” (Terms of Service, Exhibit D)
- “Policy Violations: Storage, presentation, or transmission of any material in violation of any laws, or otherwise prohibited by BurstNET®, is cause for temporary account deactivation, server/service termination, or complete cancellation of all account services. The BurstNET® Abuse Dept will make an attempt to contact the involved client via email when the first sign of a possible

violation is noted. This notification may occur before or after a service is disabled. Alerts are provided as a courtesy. Prompt responses to alerts are required. When an alert is sent, the designated abuse contact is responsible for acknowledging his/her understanding of the offense and providing an adequate response, to the satisfaction of BurstNET®, within 24 hours of the notice. Failure to sufficiently respond to an abuse alert will lead to suspension of any active services involved in abusive activity and will result in a \$50.00 fee. If reactivation is warranted, all abuse fees and any outstanding service fees must be paid prior to service being reactivated. Repeated abuse and/or failure to respond to abuse alerts will result in service termination.” (Terms of Service, Exhibit D)

- “Notwithstanding the foregoing, BurstNET® may immediately block Client's site or immediately terminate Client's access to and use of BurstNET® services and software; if at BurstNET's® sole discretion, it deems any information contained in Client's site to violate BurstNET's® Terms of Service (TOS), BurstNET's® Basic Policy and Service Guidelines (AUP), or to be otherwise objectionable or offensive or to violate the law, in accordance with Section 4.5 herein. [...] BurstNET® may terminate immediately any Client who misuses or fails to abide by this Agreement, BurstNET's™ Terms of Service (TOS), or BurstNET's™ Basic Policy and Service Guidelines (AUP) BurstNET® may terminate without notice Client's access to and use of the BurstNET® service and software upon a breach of this Agreement.” (Terms of Service, Exhibit A, ¶7.3)

35. Based on my pasted experience and on information and belief, the other web hosting services used by Defendants prohibit similar unlawful conduct.

III. THE COLLECTION AND STORAGE OF SEIZED MATERIAL

36. Plaintiffs have retained Stroz Friedberg, LLC to act as substitute custodian of any and all properties seized pursuant to the [Proposed] *Ex Parte* Temporary Restraining Order, Seizure Order And Order To Show Cause Re Preliminary Injunction. Forensic specialists employed by Stroz Friedberg will accompany Plaintiffs' representatives and the United States Marshals to each location at which the computer resources, command and control software, and other components are to be seized, and the Stroz Friedberg forensic specialists will assist the United States Marshals in identifying, collecting, and preserving the items to be seized.

37. Stroz Freidberg has particular experience in identifying, collecting, and preserving material relating to computer botnets. Plaintiff Microsoft retained Stroz Freidberg in *Microsoft Corporation v. John Doe I-11*, Case No. 2:11-cv-00222 (W.D. Wa.

2011) (Robart, J.) to identify, collect, and to preserve material related to the Rustock Botnet. Stroz Freidberg accompanied representatives of Microsoft and the United States Marshals to six locations in order to assist in the execution of a similar *ex parte* temporary restraining order and seizure order related to the Rustock Botnet.

IV. OTHER AUTHORITY AND EVIDENCE

38. Attached hereto as Exhibit 8 is a true and correct copy of the June 2, 2009 *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).

39. Attached hereto as Exhibit 9 is a true and correct copy of the June 15, 2009 Preliminary Injunction in the matter *FTC v. Pricewert LLC et al.*, Case No. 09-2407 (N.D. Cal., Whyte J.).

40. Attached hereto as Exhibit 10 is a true and correct copy of the Indictment and supporting materials in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. 2005).

41. Attached hereto as Exhibit 11 is a true and correct copy of the Sentencing in the criminal case *U.S. v. Ancheta*, Case No. 05-1060 (C.D. Cal. May 8, 2006).

42. Attached hereto as Exhibit 12 is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va., Brinkema J.).

43. Attached hereto as Exhibit 13 is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va., Brinkema J.).

44. Attached hereto as Exhibit 14 is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft v. John Does 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

45. Attached hereto as Exhibit 15 is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. John Doe 1-11*, Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.).

46. Attached hereto as Exhibit 16 is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

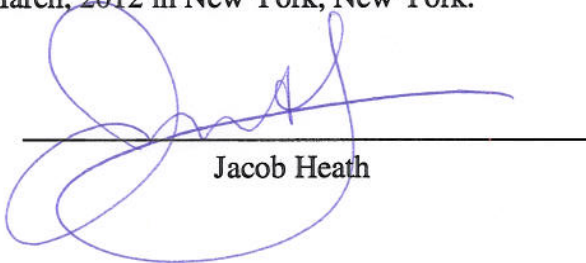
47. Attached hereto as Exhibit 17 is a true and correct copy of the Preliminary Injunction in the matter *Microsoft Corporation v. Dominique Alexander Piatti et al.*, Case No. 1:11-cv-01017 (E.D. Va. 2011) (Cacheris, J.).

48. Attached hereto as Exhibit 18 is a true and correct copy of a March 5, 2012 report entitled "White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets."

49. Attached hereto as Exhibit 19 is a true and correct copy of ICANN's "Guidance for Preparing Domain Name Orders, Seizures & Takedowns."

I declare under penalty of perjury under the laws of the United States of America and the State of New York that the foregoing is true and correct to the best of my knowledge.

Executed this 19th day of March, 2012 in New York, New York.



Jacob Heath

EXHIBIT 1.

Contents

1. Objective	1
2. Approach.....	2
3. Inputs.....	2
4. Outputs.....	8
5. References.....	10

WHOIS Proxy / Privacy Service Abuse Study –Definition

This study will measure how often domains associated with illegal or harmful Internet communication abuse Privacy/Proxy services to obscure the perpetrator's identity.

1. Objective

This study is intended to help the ICANN community determine the extent to which Proxy and Privacy services are abused during illegal or harmful Internet communication. Specifically, it will attempt to prove/disprove the following hypothesis:

A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity.

As defined by [1], "illegal or harmful communication" refers to online activities (e.g., email messages, web transactions, file downloads) that violate criminal or civil law or which harm their targets (e.g., email/download recipients, website visitors). These activities include unsolicited commercial bulk email (spam), online intellectual property or identity theft, email harassment or stalking, phishing websites, online malware dissemination, and cybersquatting. Further examples include DoS attacks, DNS cache poisoning, pirated software (warez) distribution sites, money laundering email (mules scams), advanced fee fraud email (411 scams), and online sale of counterfeit merchandise or pharmaceuticals.

Allegations of actionable harm may require victims, law enforcement officials, and others to contact domain users (i.e., owners or licensees). To facilitate identification and contact, section 3.3.1 of the ICANN Registrar Accreditation Agreement (RAA) [4] requires Registrars to provide an interactive web page and a port 43 WHOIS service to enable free access to up-to-date data concerning all active registered domain names. This WHOIS data includes the name and postal address of the Registered Name Holder and technical and administrative contacts for the domain.

According to [1], Proxy and Privacy registration services provide anonymity or privacy protection for domain users. *Privacy* services hide certain user details from WHOIS by offering alternate contact information and mail forwarding services while not actually shielding the user's identity. *Proxy* services have a third-party register domain names on

WHOIS Proxy/Privacy Abuse Study

the user's behalf and then license the use of the domain name so that a third-party's contact information (and not the licensee's) is published in WHOIS. According to the WHOIS Privacy/Proxy Prevalence Study [3], approximately 15 to 25 percent of gTLD domain names are likely to be registered using a Privacy or Proxy service.

Study proposals [8][9][10] suggest that Privacy/Proxy services are being abused to obscure the identity of perpetrators that instigate illegal or harmful Internet communication, thereby impeding investigation. For example, proposal [8] indicates that Privacy/Proxy registrations lengthen phishing website take-down times. Proposal [9] indicates that Privacy/Proxy services are being abused to shield cyber squatters (i.e., parties that register or use a domain name in bad faith to profit from someone else's trademark).

A recent study of 384 domains hosted by ISP 3FN (shut down in June 2009 for abetting criminal activity) found that 38 percent were registered to Proxy services [11]. Of those, approximately half were associated with least one kind of illegal activity. Although small and informal, this study illustrated that domains used by criminals do use Proxy services – in this case, more often than the random domains studied by [3].

To provide the ICANN community with empirical data to evaluate such concerns, this study will methodically analyze a large, broad sample of domains associated with various kinds of illegal or harmful Internet activities. It will measure how often these alleged “bad actors” abuse Privacy/Proxy services, comparing rates for each kind of activity to overall Privacy/Proxy rates measured by [3]. If those rates are found to be significant, policy changes may be warranted to deter Privacy/Proxy abuse.

Note: This study will NOT measure the frequency of illegal/harmful Internet activity. This study will gather a representative sample of illegal/harmful incidents to measure how often Privacy/Proxy services are abused by perpetrators (alleged and confirmed).

2. Approach

This hypothesis will be tested by performing a descriptive study on a representative sample of domains within the top five gTLDs (.biz, .com, .info, .net, .org). To focus on study goals, this sample will be composed exclusively of domains involved in illegal or harmful Internet communication, as documented by organizations that routinely track, investigate, and/or remediate various kinds of activities. To measure frequency of abuse, this study will divvy sampled domain users into those that can be reached directly using WHOIS data and those that must be contacted via a referenced Privacy/Proxy service.

Because creating a single sample that proportionally represents every major kind of illegal or harmful Internet communication is unrealistic, subsamples will be created for each activity to be studied (e.g., a spam sender list, a warez site list). Many domains are likely to be associated with multiple activities and may thus appear in more than one subsample. However, rates will be measured independently for each subsample to determine which activities most often abuse Privacy/Proxy services.

WHOIS Proxy/Privacy Abuse Study

Furthermore, because the nature and duration of illegal/harmful Internet activities varies, different methods will be required for incident tracking, investigation, and remediation.

- Timely response is essential for extremely **short-lived activities** (e.g., spam, phishing, DoS attacks). Where possible, domain subsamples for these activities will be generated by monitoring **live-feeds** (e.g., real-time blacklists), letting researchers query and record WHOIS data in near-real-time.
- Timely response is less critical for activities associated with **long-lived activities** (e.g., trademark infringement, cybersquatting). Subsamples for these activities would be impossible to generate in near-real-time; live-feeds do not exist. Instead, these domains and WHOIS data will be **recorded over time** by study participants routinely involved in these incidents (e.g., first responders and real-time cybercrime researchers, complaint centers and law enforcement agencies, victim advocates).

To meet this study's goals, Privacy/Proxy determination must be based on WHOIS data as it was at the time of the incident. WHOIS queries usually return Registrant data long after an offending domain's web, file, or mail servers disappear, appear on an RBL, or are taken down. However, WHOIS data may well change following illegal activity, such as when a malicious domain is suspended or re-registered. Study goals can still be met so long as a significant percentage of WHOIS queries performed shortly after incidents do not return recently-updated or no Registrant data.

Note that other WHOIS studies [3][6][7] have been defined to measure the overall frequency of Privacy/Proxy use, what types of entities (e.g., natural or legal persons) commonly use Privacy/Proxy-registered domains and for what apparent purpose (e.g., personal or commercial), and how Privacy/Proxy providers respond to domain user reveal requests. Those questions are therefore outside the scope of this study.

However, overall frequency of Privacy/Proxy use [3] must be considered when sizing this study's subsamples so that they represent the top 5 gTLD domain population with a 95% confidence interval. Furthermore, because harmful/illegal Internet communication tends to originate from certain countries and regions, live-feeds and incident reports may be geographically skewed. To reflect world-wide experiences, subsamples must be generated from input sources with international scope – for example, global RBLs.

Finally, this study should build upon the foundation laid by the WHOIS Accuracy Study [2] and WHOIS Privacy/Proxy Prevalence Study [3] as follows.

- **Sample Cleaning and Coding:** WHOIS data for every domain name must include certain mandatory values (e.g., Registrant Name), but there is no RFC-standard record format or even a single global database from which WHOIS data can be obtained. The Accuracy Study [2] developed a methodology for cleaning sampled domain WHOIS data to eliminate parsing errors, translate non-ASCII characters, map Registrants to country code/name, and sort the sample by Regional Internet Registry.

WHOIS Proxy/Privacy Abuse Study

- **Registrant Type Classification:** Next, based on WHOIS Registrant Name and Organization values, the Accuracy Study assigned each sampled domain one of the following Apparent Registrant Types: name completely missing or patently false, a natural person, an organization with or without a person's name, a multiple domain name holder (ISP or reseller), or a potential Privacy/Proxy service provider. All potential Privacy/Proxy service providers were then either confirmed or reclassified.

Even though this study's sample design process and parameters differ, researchers are strongly encouraged to apply the same sample cleaning, coding, and classification process to reduce cost and promote consistency across all WHOIS studies. In particular, the Accuracy Study's methodology for confirming potential Privacy/Proxy use should be applied, as this is the key differentiator upon which this study's findings will be based.

3. Inputs

The first step in conducting this study will be to generate subsamples of domain names associated with each kind of illegal or harmful Internet communication to be measured. As noted in Section 2, because activity nature and duration varies, this study will employ two different research methods: Live-Feed Monitoring for incidents typically reported in real-time and Offline Third-Party Recording for all other kinds of incidents.

Method 1: Live-Feed Monitoring

Domain names associated with the following short-lived illegal/harmful Internet activities should ideally be collected from live-feed sources. Possible sources are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this source list during the first phase of the study.

As alleged "bad actors" are identified from live-feeds, reverse DNS lookups and WHOIS queries will be performed in near-real-time¹ to record the Registrant's Name, Organization, and Address for domain names associated with each incident. Note that "associated domain name" depends upon the type of activity (e.g., spam sender, phishing website, malware server).

Note that, after incident investigation, many alleged bad actors do not end up being the real perpetrators. For example, many spam senders and phishing servers will be "bots" -- compromised hosts used by criminals without the Registrant's knowledge. Furthermore, domains may be added to RBLs based on complaints rather than verified incidents.

However, these "false positive" incident reports still require investigation; WHOIS Registrant data for those domains plays a role in enabling (or inhibiting) investigation. Therefore, this study must gather and analyze the WHOIS data associated with *all* alleged bad actors (proven or otherwise). To avoid skewing results, this study will *also* analyze refined samples that have been filtered to weed out low-probability cases – for example,

¹ Researchers will need to work around port 43 rate limits by pacing WHOIS queries, retrying failed queries, arranging for preferential access from a WHOIS query provider, or enlisting the help of a live-feed supplier that already has preferential access.

WHOIS Proxy/Privacy Abuse Study

eliminating domains associated with fewer than N reported incidents. Objective sample filtering methods should be defined by researchers at study start; suggestions are welcome.

Once sufficiently large subsamples have been collected for each activity, they will be cleaned, coded, and classified by Registrant Type as described in Section 2 for statistical analysis as described in Section 4.

- **Spam:** Live-feeds from several major real-time Domain Name System Blacklists ([DNSBLs](#)) could be used to generate a subsample of spam sender IP addresses/ranges and associated unique domain names. Possible sources include [Spamhaus](#) Blocklist, [Mailshell](#) Live-Feed, [SURBL](#), [URIBL](#), and [SORBS](#) DNSBL.
- **Phishing:** Several major Phishing website live-feeds could be used to generate a subsample of phishing URLs and the domain names that host them. Possible sources include OpenDNS [PhishTank](#) and Internet Identity [RealPhish](#).
- **Malware:** A subsample of domains used to host and disseminate malware could be created from live-feeds maintained by major malware researchers and/or Internet security vendors. Possible sources include SRI [Malware Threat Center](#), [FireEye](#) Malware Analysis & Exchange, and [Malware Domains](#).
- **Denial-of-Service and DNS Cache Poisoning:** Input is requested on live-feed sources that could be used to generate subsamples of domains that send harmful messages during these time-sensitive attacks. Potential sources include the [IMPACT Global Response Centre](#) NEWS feed and [FIRST](#)-member incident response teams.

Method 2: Offline Third-Party Recording

Domain names associated with less time-critical illegal/harmful activities will be gathered from third-parties that routinely respond to or track such incidents in large volume and might be willing to assist by recording WHOIS data early in their investigation. Candidates include first responders and real-time cybercrime researchers, Internet crime complaint centers and law enforcement agencies, and victim advocates. Possible participants are listed below; additional suggestions are welcome. Researchers are expected to refine and finalize this participant list during the first phase of the study.

Consistency and accuracy of reported data is always a concern whenever numerous independent parties supply input for aggregate statistical analysis. To address this concern, researchers will develop a short, simple incident reporting form and process that participants can use to record the type of illegal/harmful activity, associated domain name, and WHOIS Registrant Name, Organization, and Address in a timely fashion. Here again, note that "associated domain name" depends upon the type of activity (e.g., phishing website, warez server, money laundering email sender).

At study start, researchers will identify and invite representative sources to participate. All participants must agree to record and report all incidents encountered as part of their

WHOIS Proxy/Privacy Abuse Study

normal operation during a specified study period (e.g., 30 days). In particular, participants shall be asked to report all alleged perpetrators (proven or otherwise), and to indicate whether investigation confirmed or refuted their alleged involvement in the incident. This data collection approach makes it possible to study both the entire sample and a refined sample, filtered to focus on high-probability bad actors.

Although these longer-lived incidents may not be as time-sensitive as those monitored by live-feed, participants must still perform reverse DNS lookups and WHOIS queries on alleged perpetrator IP addresses and domain names as soon as possible after incidents are detected, not at the end of the study period.

A submission process will be designed to minimize participant effort while promoting consistent, accurate reporting. After a sufficiently large/broad set of third-party reports have been submitted, researchers will clean, code, and classify WHOIS data by Registrant Type as described in Section 2 for analysis as described in Section 4.

- **Phishing:** In proposal [8], the Anti Phishing Working Group ([APWG](#)) offered to supply a global list of phishing URLs, domains used to host them, and associated shutdown times. Due to the short duration of phishing sites, live-feed monitoring is preferable. However, analyzing this activity with both research methods might be useful to determine whether results differ significantly.
- **Cybersquatting:** Data on domains cited in alleged cybersquatting incidents might be gathered by organizations like the International Trademark Association ([INTA](#)). Approved dispute resolution service providers involved in ICANN's Uniform Domain-Name Dispute Resolution Policy ([UDRP](#)) are another possible source, although waiting until a dispute is filed to query WHOIS may be too much delay.
- **Intellectual property theft:** Data on domains cited in intellectual property theft complaints might be gathered by organizations like the UK [Alliance Against IP Theft](#) or the International Intellectual Property Rights ([IPR](#)) Advisory Program. However, data might be more readily available from groups that routinely record and investigate specific kinds of IP theft complaints, described below.
- **Media Piracy:** Data on domain names used by servers that illegally share copyrighted movies and music might be gathered by The International Federation of the Phonographic Industry ([IFPI](#)), the Motion Picture Association of America ([MPAA](#)), the Recording Industry Association of America ([RIAA](#)), and their international counterparts.
- **Software Piracy:** Data on domain names used by servers that illegally distribute copyrighted software might be gathered by major software vendors like Microsoft and Adobe or from an anti-piracy organization like the Business Software Alliance ([BSA](#)).

WHOIS Proxy/Privacy Abuse Study

- **Trademark Infringement:** Data on domain names alleged to infringe upon registered trademarks might be gathered by an organization like the International Trademark Association ([INTA](#)) or commercial first-responders like [Mark Monitor](#).
- **Counterfeit Merchandise:** Data on domains that send email advertising counterfeit merchandise and illegal pharmaceuticals might be gathered by an investigative agency like the US National Intellectual Property Rights Coordination Center Cyber Crimes Section ([CCS](#)). However, given that spam (one primary vector for online sale of counterfeit merchandise) can be studied more easily via live-feed, it might not be necessary to study this activity with method 2.
- **Money Laundering:** Data on domains that send recruiting email associated with fraudulent money laundering scams might be gathered by legitimate job recruitment websites like [Monster](#) and [HotJobs](#) or by an organization like [BobBear](#) that focuses specifically on tracking this type of illegal activity.
- **Advanced Fee Fraud:** Data on domains that send solicitation email associated with advanced fee fraud scams might be gathered by a tracking site like [Artists Against 419](#) or bodies that handle Internet fraud complaints such as the FBI/NWCC Internet Crime Complaint Center ([IC3](#)) and its counterparts in other countries.
- **Identity Theft:** Data on domains that send bait email associated with online identity thefts might be gathered by the FBI/NWCC Internet Crime Complaint Center ([IC3](#)) or the US National Intellectual Property Rights Coordination Center [Identity Fraud Initiative](#). However, major online identity theft vectors like phishing and malware can be studied more easily via live-feed monitoring; reliably correlating reported identity thefts to specific email messages and domains that caused them could be difficult.
- **Child Pornography:** Data on domain names of servers involved in online distribution of child pornography might be gathered by US National Intellectual Property Rights Coordination Center Cybercrimes Child Exploitation Section ([CES](#)) and [Operation Predator](#). However, study [11] found it hard to obtain WHOIS data for child porn domains because, not only were sites taken down, but domain names were suspended.
- **Harassment or Stalking:** Input is requested on how to obtain a representative subsample of domain names that send online harassment and cyber-stalking email. Incidents are reported to local law enforcement agencies like [FBI](#) field offices. While [HaltAbuse.org](#) tracks statistics, based upon data supplied voluntarily by victims, many victims are reluctant to disclose these crimes. The highly personal nature of these activities could make it difficult to obtain a representative subsample.
- **Other Cybercrimes:** The FBI/NWCC Internet Crime Complaint Center ([IC3](#)) might also be able to supply data on perpetrator domains cited in complaints by victims of other cybercrimes, including online auction, investment fraud, and Internet extortion.

WHOIS Proxy/Privacy Abuse Study

Because domain subsamples are likely to have some degree of cross-over, other readily-available online resources can be consulted to confirm and expand upon the kinds of illegal or harmful Internet communication associated with each domain. For example, in addition to RBLs, study [11] searched for domains using ReputationAuthority.org, Google Safe Browsing, McAfee SiteAdvisor, and Malware Domain List (either by searching a published list or by attempting to browse a website).

For each sampled domain, an **Apparent Registrant Type** must be assigned using the methodology defined by the WHOIS Accuracy Study [2], including confirmation of all domains potentially registered using Privacy/Proxy services. After this classification has been completed, the following input data will be available for each sampled domain:

Raw Data recorded by monitoring live-feed or reported by study participants

- Domain Name
- Registrant Name (may be a Privacy/Proxy service)
- Registrant Organization (may be a Privacy/Proxy service)
- Full WHOIS record for the domain
- Number of Illegal or Harmful Activity reported for this domain
- Kind(s) of Illegal or Harmful Activity reported for this domain
- Input Source(s) which supplied this domain name
- Incident Investigation Outcome (confirmed, refuted, in-progress/unknown)

Additional Data supplied by researchers

- Apparent Registrant Country Code/Name
- Apparent Registrant Type: missing/false, natural person, organization, multiple domain holder, or Privacy/Proxy service provider
- Additional Kind(s) of Illegal or Harmful Activity associated with this domain, as determined by searching RBLs and site reputation lists

4. Outputs

This study will quantify the frequency of Privacy/Proxy use among domains allegedly involved in illegal or harmful communication, broken down by kind of activity. To deliver these empirical results, this study will examine the WHOIS Registrant data associated with each sampled domain as follows.

- During classification, some domains will be found to have missing, patently false, or otherwise unusable WHOIS Registrant data, thereby impeding perpetrator identification. These domains represent another method of WHOIS abuse which should be measured and included in study findings, but do not constitute Privacy/Proxy abuse.
- During classification, some domains will be found to have WHOIS Registrant data that explicitly identifies and supplies direct contact information for a natural person, an organization (with or without a person's name), or a multiple domain holder. These Registrants may or may not actually be responsible for the reported

WHOIS Proxy/Privacy Abuse Study

illegal or harmful communication. For example, many domain names will be mapped to spambot-compromised residential broadband hosts or trojan-hacked websites operated by legitimate businesses. However, for the purposes of this study, the users of these domains shall be considered readily-identifiable and directly-contactable using Registrant data returned from a simple WHOIS query.

- The rest of the sample will consist of domains that, following classification, have WHOIS Registrant data that identifies an apparent Privacy/Proxy provider. For the purposes of this study, all such domains will be considered to have abused a Privacy/Proxy service for the purpose of obscuring perpetrator identification. To determine significance, this abuse rate shall be compared to the overall rate of Privacy/Proxy use measured by [3] (15-25%).

For each kind of activity studied, the following measurements will be derived from the entire subsample of alleged bad actors (including bots and other false positives):

- Percentage of entire sample that could not be analyzed, categorized by reason (e.g., false/missing WHOIS, recently modified WHOIS, suspended domain)
- Percentage of entire sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of entire sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of entire sample apparently registered via Proxy service, distributed by gTLD/country

For each kind of activity studied, similar measurements will also be derived from a refined subsample, filtered to reduce false positives and focus on confirmed bad actors:

- Percentage of refined sample that could not be analyzed, categorized by reason
- Percentage of refined sample with Registrant NOT obscured via Privacy/Proxy, distributed by gTLD/country
- Percentage of refined sample apparently registered via Privacy service, distributed by gTLD/country
- Percentage of refined sample apparently registered via Proxy service, distributed by gTLD/country

Finally, these results will be aggregated and used to answer the following questions:

- Are Privacy services abused more/less often by bad actors (alleged or confirmed)?
- Are Proxy services abused more/less often by bad actors (alleged or confirmed)?
- Which illegal/harmful activities are most likely to abuse Privacy/Proxy services?
- Which illegal/harmful activities are least likely to abuse Privacy/Proxy services?
- Were there any kinds of illegal/harmful Internet communication for which Privacy/Proxy abuse could not be studied in a reliable way and why?

5. References

- [1] [Working Definitions for Key Terms that May be Used in Future WHOIS Studies](#), GNSO Drafting Team, 18 February 2009
- [2] [Proposed Design for a Study of the Accuracy of Whois Registrant Contact Information](#) (6558,6636), NORC, June 3, 2009
- [3] [ICANN's Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs](#), ICANN, September 28, 2009
- [4] [Registrar Accreditation Agreement \(RAA\)](#), ICANN, 21 May 2009
- [5] [Terms of Reference for WHOIS Misuse Studies](#), ICANN, September 2009
- [6] [Terms of Reference for WHOIS Registrant Identification Studies](#), ICANN, Oct 2009
- [7] [Terms of Reference for WHOIS Privacy/Proxy Reveal Studies](#), ICANN, In Progress
- [8] [Study Suggestion Number 13b/c](#), Measure growth of proxy/privacy services vis-à-vis all registrations, Laura Mather
- [9] [Study Suggestion Number Study 17](#), Identify why proxy/privacy service users use those services, Claudio DiGangi
- [10] [GAC Data Set 11](#), What is the percentage of domain names registered using proxy or privacy services that have been associated with fraud or other illegal activity, GAC Recommendations for WHOIS Studies, 16 April 2008
- [11] [Private Domain Registrations](#): Examining the relationship between private domain registrations and malicious domains at 3FN, Piscitello, October 2009

EXHIBIT 2.

What Does ICANN Do?

Deutsch (/de/about/participate/what)	Español (/es/about/participate/what)	Français (/fr/about/participate/what)
Italiano (/it/about/participate/what)	日本語 (/ja/about/participate/what)	한국어 (/ko/about/participate/what)
Português (/pt/about/participate/what)	Русский (/ru/about/participate/what)	简体中文 (/zh/about/participate/what)
	العربية (/ar/about/participate/what)	

To reach another person on the Internet you have to type an address into your computer - a name or a number. The address has to be unique so computers know where to find each other. ICANN (Internet Corporation for Assigned Names and Numbers) coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

ICANN (Internet Corporation for Assigned Names and Numbers) was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

ICANN (Internet Corporation for Assigned Names and Numbers) doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system it does have an important impact on the expansion and evolution of the Internet.

What is the domain name system?

The domain name system, or DNS (Domain Name System), is a system designed to make the Internet accessible human beings. The main way computers that make up the Internet find one another is through a series of numbers, with each number (called an "IP (Intellectual Property; or Internet Protocol) address") correlating to a different device. However it is difficult for the human mind to remember long lists of numbers so the DNS (Domain Name System) uses letters rather than numbers, and then links a precise series of letters with a precise series of numbers.

The end result is that ICANN (Internet Corporation for Assigned Names and Numbers)'s website can be found at "icann.org" rather than "192.0.34.163" – which is how computers on the network know it. One advantage to this system – apart from making the network much easier to use for people – is that a particular domain name does not have to be tied to one particular computer because the link between a particular domain and a particular IP (Intellectual Property; or Internet Protocol) address can be changed quickly and easily. This change will then be recognised by the entire Internet within 48 hours thanks to the constantly updating DNS (Domain Name System) infrastructure. The result is an extremely flexible system.

A domain name itself comprises two elements: before and after "the dot". The part to the right of the dot, such as "com", "net", "org" and so on, is known as a "top-level domain" or TLD (Top Level Domain). One company in each case (called a registry), is in charge of all domains ending with that particular TLD (Top Level Domain) and has access to a full list of domains directly under that name, as well as the IP (Intellectual Property; or Internet Protocol)

addresses with which those names are associated. The part before the dot is the domain name that you register and which is then used to provide online systems such as websites, email and so on. These domains are sold by a large number of “registrars”, free to charge whatever they wish, although in each case they pay a set per-domain fee to the particular registry under whose name the domain is being registered.

ICANN (Internet Corporation for Assigned Names and Numbers) draws up contracts with each registry*. It also runs an accreditation system for registrars. It is these contracts that provide a consistent and stable environment for the domain name system, and hence the Internet.

In summary then, the DNS (Domain Name System) provides an addressing system for the Internet so people can find particular websites. It is also the basis for email and many other online uses.

What does ICANN (Internet Corporation for Assigned Names and Numbers) have to do with IP (Intellectual Property; or Internet Protocol) addresses?

ICANN (Internet Corporation for Assigned Names and Numbers) plays a similar administrative role with the IP (Intellectual Property; or Internet Protocol) addresses used by computers as it does with the domain names used by humans. In the same way that you cannot have two domain names the same (otherwise you never know where you would end up), for the same reason it is also not possible for there to be two IP (Intellectual Property; or Internet Protocol) addresses the same.

Again, ICANN (Internet Corporation for Assigned Names and Numbers) does not run the system, but it does help coordinate how IP (Intellectual Property; or Internet Protocol) addresses are supplied to avoid repetition or clashes.

ICANN (Internet Corporation for Assigned Names and Numbers) is also the central repository for IP (Intellectual Property; or Internet Protocol) addresses, from which ranges are supplied to regional registries who in turn distribute them to network providers.

What about root servers?

Root servers are a different case again. There are 13 root servers – or, more accurately, there are 13 IP (Intellectual Property; or Internet Protocol) addresses on the Internet where root servers can be found (the servers that have one of the 13 IP (Intellectual Property; or Internet Protocol) addresses can be in dozens of different physical locations).

These servers all store a copy of the same file which acts as the main index to the Internet’s address books. It lists the address for each top-level domain (.com, .de, etc) where that registry’s own address book can be found.

In reality, the root servers are consulted fairly infrequently (considering the size of the Internet) because once computers on the network know the address of a particular top-level domain they retain it, checking back only occasionally to make sure the address hasn’t changed. Nonetheless, the root servers remain vital for the Internet’s smooth functioning.

The operators of the root servers remain largely autonomous, but at the same time work with one another and with ICANN (Internet Corporation for Assigned Names and Numbers) to make sure the system stays up-to-date with the Internet’s advances and changes.

What is ICANN (Internet Corporation for Assigned Names and Numbers)’s role?

As mentioned earlier, ICANN (Internet Corporation for Assigned Names and Numbers)’s role is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.

This is commonly termed “universal resolvability” and means that wherever you are on the network – and hence the world – that you receive the same predictable results when you access the network. Without this, you could end up with an Internet that worked entirely differently depending on your location on the globe.

How is ICANN (Internet Corporation for Assigned Names and Numbers) structured?

ICANN (Internet Corporation for Assigned Names and Numbers) is made up of a number of different groups, each of which represent a different interest on the Internet and all of which contribute to any final decisions that ICANN

(Internet Corporation for Assigned Names and Numbers)'s makes.

There are three "supporting organisations" that represent:

- The organisations that deal with IP (Intellectual Property; or Internet Protocol) addresses
- The organisations that deal with domain names
- The managers of country code top-level domains (a special exception as explained at the bottom).

Then there are four "advisory committees" that provide ICANN (Internet Corporation for Assigned Names and Numbers) with advice and recommendations. These represent:

- Governments and international treaty organisations
- Root server operators
- Those concerned with the Internet's security
- The "at large" community, meaning average Internet users.

And finally, there is a Technical Liaison Group, which works with the organisations that devise the basic protocols for Internet technologies.

ICANN (Internet Corporation for Assigned Names and Numbers)'s final decisions are made by a Board of Directors. The Board is made up of 21 members: 15 of which have voting rights and six are non-voting liaisons. The majority of the voting members (eight of them) are chosen by an independent Nominating Committee and the remainder are nominated members from supporting organisations.

ICANN (Internet Corporation for Assigned Names and Numbers) then has a President and CEO who is also a Board member and who directs the work of ICANN (Internet Corporation for Assigned Names and Numbers) staff, who are based across the globe and help co-ordinate, manage and finally implement all the different discussions and decisions made by the supporting organisations and advisory committees. An ICANN (Internet Corporation for Assigned Names and Numbers) Ombudsman acts as an independent reviewer of the work of the ICANN (Internet Corporation for Assigned Names and Numbers) staff and Board.

How does ICANN (Internet Corporation for Assigned Names and Numbers) make decisions?

When it comes to making technical changes to the Internet, here is a simplified rundown of the process:

Any issue of concern or suggested changes to the existing network is typically raised within one of the supporting organisations (often following a report by one of the advisory committees), where it is discussed and a report produced which is then put out for public review. If the suggested changes impact on any other group within ICANN (Internet Corporation for Assigned Names and Numbers)'s system, that group also reviews the suggested changes and makes its views known. The result is then put out for public review a second time.

At the end of that process, the ICANN (Internet Corporation for Assigned Names and Numbers) Board is provided with a report outlining all the previous discussions and with a list of recommendations. The Board then discusses the matter and either approves the changes, approves some and rejects others, rejects all of them, or sends the issue back down to one of the supporting organisations to review, often with an explanation as to what the problems are that need to be resolved before it can be approved.

The process is then rerun until all the different parts of ICANN (Internet Corporation for Assigned Names and Numbers) can agree a compromise or the Board of Directors make a decision on a report it is presented with.

How is ICANN (Internet Corporation for Assigned Names and Numbers) held accountable?

ICANN (Internet Corporation for Assigned Names and Numbers) has external as well as internal accountabilities.

Externally, ICANN (Internet Corporation for Assigned Names and Numbers) is an organisation incorporated under the

law of the State of California in the United States. That means [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) must abide by the laws of the United States and can be called to account by the judicial system i.e. [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) can be taken to court.

[ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) is also a non-profit public benefit corporation and its directors are legally responsible for upholding their duties under corporation law.

Internally, [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) is accountable to the community through

- Its bylaws
- The representative composition of the [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) Board from across the globe
- An independent Nominating Committee that selects a majority of the voting Board members
- Senior staff who must be elected annually by the Board
- Three different dispute resolution procedures (Board reconsideration committee; Independent Review Panel; Ombudsman)

The full range of [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#)'s accountability and transparency frameworks and principles (</en/accountability/frameworks-principles/contents-overview.htm>) are available online.

* There is an important exception to this in the form of “country code top-level domains” (ccTLDs) such as .de for Germany or .uk for the United Kingdom. There are over 250 ccTLDs, some of which have a contract with [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#); others of which have signed working agreements with [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#); and some of which have yet to enter any formal agreement with [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#). [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) however does carry out what is known as the “[IANA \(Internet Assigned Numbers Authority\)](#) function” in which every ccTLD (Country Code Top Level Domain)'s main address is listed so the rest of the Internet can find it. [ICANN \(Internet Corporation for Assigned Names and Numbers\)](#) is also in the position where it can add new TLDs to the wider system, as it did in 2000 and 2004 when seven and six new TLDs respectively were “added to the root”.

[Welcome \(/en/about/welcome\)](/en/about/welcome)

[Learning \(/en/about/learning\)](/en/about/learning)

[Participate \(/en/about/participate\)](/en/about/participate)

[What ICANN Does \(/en/about/participate/what\)](/en/about/participate/what)

[Effect on the Internet \(/en/about/participate/effect\)](/en/about/participate/effect)

[What's Going On Now \(/en/about/participate/now\)](/en/about/participate/now)

[How to Participate \(/en/about/participate/how\)](/en/about/participate/how)

[Fellowships \(/en/about/participate/fellowships\)](/en/about/participate/fellowships)

[Board \(http://www.icann.org/en/groups/board\)](http://www.icann.org/en/groups/board)

[CEO \(/en/groups/board/beckstrom.htm\)](/en/groups/board/beckstrom.htm)

[Staff \(/en/about/staff\)](/en/about/staff)

[Careers \(https://icann-openhire.silkroad.com/epostings/index.cfm?fuseaction=app.allpositions&company_id=16025&version=1 \)](https://icann-openhire.silkroad.com/epostings/index.cfm?fuseaction=app.allpositions&company_id=16025&version=1)

[Governance \(/en/about/governance\)](/en/about/governance)

[A Unique Authoritative Root \(/en/about/unique-authoritative-root\)](/en/about/unique-authoritative-root)

[Agreements \(/en/about/agreements\)](/en/about/agreements)

[Accountability & Transparency \(http://www.icann.org/en/news/in-focus/accountability\)](http://www.icann.org/en/news/in-focus/accountability)

[AOC Review \(/en/about/aoc-review\)](/en/about/aoc-review)

[Annual Report \(/en/about/annual-report\)](/en/about/annual-report)

[Financials \(/en/about/financials\)](/en/about/financials)

[Document Disclosure \(/en/about/transparency\)](/en/about/transparency)

[Planning \(/en/about/planning\)](/en/about/planning)

Stay Connected

© 2012 Internet Corporation For Assigned Names and Numbers. [Press \(/news/press\)](/news/press) | [Site map \(/sitemap\)](/sitemap)