

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-82, CONTROLLING A
COMPUTER BOTNET THEREBY
INJURING MICROSOFT AND ITS
CUSTOMERS,

Defendants.

FILED UNDER SEAL

Civil Action No. _____

**DECLARATION OF JEFFREY L. COX IN
SUPPORT OF MICROSOFT'S *EX PARTE*
APPLICATION FOR AN EMERGENCY
TEMPORARY RESTRAINING ORDER,
SEIZURE ORDER AND ORDER TO
SHOW CAUSE RE PRELIMINARY
INJUNCTION**

I, Jeffrey L. Cox, declare as follows:

1. I am an attorney with the law firm of Orrick, Herrington & Sutcliffe LLP ("Orrick"), counsel of record for Plaintiff Microsoft Corporation ("Microsoft"). I make this declaration in support of Microsoft's 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.

2. Microsoft seeks an *Ex Parte* Temporary Restraining Order, Seizure Order, And Order To Show Cause Re Preliminary Injunction to disable the Internet domains and the Internet Protocol ("IP") addresses and to seize the command and control servers and software used by the John Doe Defendants ("Defendants") to operate the Citadel 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 Microsoft, I have participated in Microsoft's previous efforts to disable other computer botnets including the "Waledac" Botnet in February 2010 in the Eastern District of Virginia, the "Rustock" Botnet in March 2011 in the Western District of Washington, the "Kelihos" Botnet in September 2011 in the Eastern District of Virginia, the "Zeus" Botnets in March 2012 in the Eastern District of New York, the "Nitol" Botnet in September 2012 in the Eastern District of Virginia, and the "Bamital" Botnet in January 2013 in the Eastern District of Virginia. 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.

1. Microsoft's 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. Microsoft has not sought previously this particular *ex parte* relief in the United States District Court for the Western District of North Carolina as to these Defendants.

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

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

4. 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, e-mail 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.

5. 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 e-mail 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 e-mail 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 e-mail 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.”

6. Based on my prior experience and from my research, I believe that the most reliable contact information for effecting communication with Defendants are e-mail addresses and messaging addresses that have been discovered to be associated with defendants and the contact information, particularly e-mail addresses, in possession of the domain registries and web hosting companies. From my research, I conclude that such contact information is likely to be an effective means of communicating with Defendants, 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 Microsoft, notice of this proceeding and service of process may be attempted using such contact information. Through my research, I have also determined that Defendant John Doe 1 has used an alias on the Jabber instant messaging service. 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.

I. NOTICE AND SERVICE OF PROCESS

A. Microsoft Has Robust Plans To Provide Notice

7. On behalf of Microsoft, 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, or instant messaging service.

8. On behalf of Microsoft, 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.botnetlegalnotice.com/citadel>. 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: “Plaintiff Microsoft Corporation (“Microsoft”) has sued defendants John Does 1-82 associated with the Internet Domains and Internet IP Addresses listed below. Microsoft alleges 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 e-mail to the injury of Microsoft and the public. Microsoft seeks 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. Microsoft seeks a permanent injunction, other equitable relief and damages. Full copies of the pleading documents are available at <http://www.botnetlegalnotice.com/citadel>.”
- 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

Microsoft's attorneys, Neil T. Bloomfield, Moore & Van Allen PLLC, 100 North Tryon Street, Suite 4700, Charlotte, NC 28202-4003; 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.”

9. On behalf of Microsoft, 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.botnetlegalnotice.com/citadel> in the local language in general circulation newspapers in Russia and Ukraine, where Defendants are generally believed to reside.

10. On behalf of Microsoft, Orrick will serve each of the Internet domain registries listed at Appendix A to the Complaint and the web hosting companies listed at Appendix B to the Complaint with copies of all documents served on Defendants.

11. On behalf of Microsoft, 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.

12. On behalf of Microsoft, 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.

13. Other than notifying the Department of Justice in Washington, DC, the United States Attorney for the Western District Of North Carolina, and the United States Marshals Service in districts where seizure is to be effected and preparing for service of process after any order is executed, pursuant to Section 1116(d)(2) of the Lanham Act, Microsoft has not and will not publicize the requested seizure until after the requested seizure is carried out.

B. Notice Under ICANN Domain Name Registration Policies

14. 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.

15. 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**.

16. 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**.

17. 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**

18. 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....”

19. 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**

20. 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.

21. 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.

22. 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 noticed does not include a hardcopy of the complaint itself or any annexes.”

23. 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...”

24. 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 e-mail addresses provided by registrants.

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

25. 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**

26. 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.”

27. 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**

28. The terms of service of 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.”

29. 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**

30. 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” (e-mails/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, e-mail address harvesting, and/or unsolicited e-mail (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 e-mail 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)

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

II. THE COLLECTION AND STORAGE OF SEIZED MATERIAL

32. Microsoft has 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 Microsoft’s 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 Federal Bureau of Investigation and the United States Marshals in identifying, collecting, and preserving the items to be seized.

33. 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 1-11*, 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.

III. OTHER AUTHORITY AND EVIDENCE

34. 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.).

35. 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.).

36. 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).

37. 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).

38. 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.).

39. 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.).

40. 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.).

41. 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.).

42. 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.).

43. 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.).

44. Attached hereto as **Exhibit 18** is a true and correct copy of the Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation et al. v. John Does 1-39*, Case No. 1:12-cv-01335 (E.D. N.Y.) (Mann, J.).

45. Attached hereto as **Exhibit 19** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft Corporation et al. v. John Does 1-39*, Case No. 1:12-cv-01335 (E.D. N.Y.) (Mann, J.).

46. Attached hereto as **Exhibit 20** is a true and correct copy of the *Ex Parte* Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation v. Peng Yong et al.*, Case No. 1:12-cv-1004 (E.D. Va. 2012) (Lee, J.).

47. Attached hereto as **Exhibit 21** is a true and correct copy of the *Ex Parte* Temporary Restraining Order and Order to Show Cause in the matter of *Microsoft Corporation v. John Does 1-18*, Case no. 1:13-cv-00139 (E.D. Va. 2013) (Brinkema, J.).

48. Attached hereto as **Exhibit 22** is a true and correct copy of the Preliminary Injunction in the matter of *Microsoft Corporation v. John Does 1-18*, Case no. 1:13-cv-00139 (E.D. Va. 2013) (Brinkema, J.).

49. Attached hereto as **Exhibit 23** is a true and correct copy of the Complaint in the matter of *United States v. John Doe 1-13*, Case No. 3:11-cv-561 (D. Ct. 2011).

50. Attached hereto as **Exhibit 24** is a true and correct copy of the Preliminary Injunction in the matter of *United States v. John Doe 1-13*, Case No. 3:11-cv-561 (D. Ct. 2011).

51. Attached hereto as **Exhibit 25** is a true and correct copy of a March 5, 2012 report entitled “White House Advisor Schmidt Discusses Online Trusted ID Plan, Fighting Botnets.”

52. Attached hereto as **Exhibit 26** 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 28th day of May, 2013


Jeffrey L. Cox