



23), Preliminary Injunction Order (Dkt. 33) and Supplemental Preliminary Injunction Order (Dkt. 49), and these Defendants have failed to plead or otherwise defend the action.

3. As of June 12, 2017, I have not been contacted by any of the Defendants regarding this case or at all. I have also conferred with Richard Boscovich, Assistant General Counsel in Microsoft's Digital Crimes Unit, who confirms that Microsoft, or any party associated with it, have not been contacted by any of the Defendants regarding this case or at all. Defendants have not objected to the relief obtained in the Temporary Restraining Order, the Preliminary Injunction Order or the Supplemental Preliminary Injunction Order, or any order of the Court Monitor. Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

4. The 21-day time for Defendants to respond to the complaint under Fed. R. Civ. P. 12 has expired, as Defendants were served on August 6, 2016 via publication and at numerous points between August 2016 and March 2017 via email. Upon information and belief, the Defendants against whom a notation of default is sought are not infants or incompetent persons. I base this conclusion on the fact that Defendants have engaged in sophisticated acts of computer intrusion and theft of sensitive information from computer networks and have operated and procured sophisticated cybercrime infrastructure. I have also seen no indication that Defendants are absent or have failed to file responsive pleadings due to present military service.

**B. Service Of Process And Notice Upon Defendants**

**1. Defendants Are Aware Of This Proceeding Given The Impact Of The TRO And Preliminary Injunction Orders**

5. I submit that it is most reasonable to conclude that Defendants are aware of this proceeding given the significant impact of the TRO and preliminary injunction orders on their operations, in combination with the steps Microsoft took to serve process by email and through publication, discussed below.

6. As attested in the Declaration of Jason Norton (Dkt. 42-1 ¶¶ 4-6), following execution of the TRO and preliminary injunction orders, traffic from the subject Internet

domains that comprised the Defendants' command and control infrastructure to infected victim operating systems and devices, was redirected to Microsoft's secure servers. As attested in the Norton Declaration, this effectively interrupted Defendants' attacks by severing communications between the infected operating systems and devices of at least 122 victims and the Defendants. (Dkt. 42-1 ¶¶ 5-6). As attested in the Norton Declaration, to attempt to recover from the loss of this infrastructure, Defendants continued to register and activate new domains for use in the same infrastructure and to target victims. (Dkt. 42-1 ¶ 6). This suggests that Defendants were aware of their loss of communications with the infected operating systems and devices and were taking steps to restore their command and control infrastructure. Microsoft blocked these attempts. Given the obvious impact on the infrastructure, I conclude that Defendants are very likely to be aware of that impact and to be aware of the fact that the instant proceeding is the cause of that impact.

**C. Service By Internet Publication**

7. Microsoft has served process by Internet publication, as authorized by the TRO, Preliminary Injunction Order and Supplemental Preliminary Injunction Order. The Court has authorized service by Internet publication, as follows: "the Complaint may be served by any means authorized by law, including... "publishing notice on a publicly available Internet website." Dkt. 23 at p. 8.

8. I personally oversaw service of process by publication, including each of the following actions, on behalf of Microsoft.

9. Beginning on August 6, 2016, I published the Complaint, summons, TRO and all associated pleadings, declaration and evidence on the publicly available website [www.noticeofpleadings.com/strontium](http://www.noticeofpleadings.com/strontium). Thereafter, I published the Preliminary Injunction Order and Supplemental Preliminary Injunction Order, and all other pleadings, declarations, evidence, orders and other submissions filed with the Court in this action on the publicly available website [www.noticeofpleadings.com/strontium](http://www.noticeofpleadings.com/strontium). All pleadings and orders filed with the Court have been made available on that website throughout the case.

10. I also included prominently at the top of the website, the following text:

“Plaintiff Microsoft Corporation (“Microsoft”) has sued Defendants John Does 1-2 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft’s customers’ computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft’s customers. Microsoft seeks a preliminary injunction directing the registries associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are 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 [www.noticeofpleadings.com/strontium](http://www.noticeofpleadings.com/strontium).

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 Microsoft attorney, Gabriel M. Ramsey at Orrick, Herrington & Sutcliffe LLP, The Orrick Building, 405 Howard Street, San Francisco, California, 94105-2669. If you have questions, you should consult with your own attorney immediately.”

11. A link to the foregoing website was included in each service of process email sent to Defendants at the email addresses determined to be associated with the Defendants’ domains used in the Strontium operations. Attached hereto as **Exhibit 1** is a true and correct copy of a screenshot of the publicly available website [www.noticeofpleadings.com/strontium](http://www.noticeofpleadings.com/strontium).

**D. Service By Email**

12. Microsoft has served process through email, as authorized by the TRO, Preliminary Injunction Order and Supplemental Preliminary Injunction Order. The Court has authorized service by email, as follows: “the Complaint may be served by any means authorized by law, including (1) transmission by email... to the contact information provided by Defendants to Defendants’ domain registrars and/or hosting companies.” Dkt. 23 at p. 8.

13. Through Microsoft’s pre-filing investigation, its in-house investigators and attorneys at Orrick, Herrington & Sutcliffe LLP gathered contact information, particularly email addresses, associated with the Defendants’ domains. Defendants had provided these email

addresses to domain registrars when completing the registration process for the domains used in Defendants' command and control infrastructure. I used this contact information to serve the Defendants by email.

14. In this case, the email addresses provided by Defendants to the domain registrars are the most accurate and viable contact information and means of notice and service. I have personally researched in detail the identifying information and mailing addresses used in the registration of the domains used by Defendants, as discussed further below. In each case, my investigation has shown that Defendants provided to the domain registrars false or stolen names, addresses, facsimile numbers and telephone numbers. However, in each case Defendants provided an operational, active email address to the domain registrars. Defendants will have expected notice regarding their use of the domains by the email addresses that they provided to their domain registrars. For example, as set forth in the Declaration of Jeffrey L. Cox at Dkt. 15 ¶¶ 16-32, ICANN domain registration policies require Defendants to provide accurate email contact information to registrars and the registrars use such information to provide notice of complaints and to send other account-related communications about the domain, including communications which result in suspension or cancellation of the domain registration.

15. Given that Defendants connected to the infected victim computers through these domains, it was crucial for them to remain vigilant as to any change of the domains' status, and the email addresses associated with the domains are the means by which they did so. For example, during the course of discovery in this action, I received subpoena responses from the email providers associated with Defendants' email addresses which show that the domain registrars often sent communications, including renewal and billing notices and other communications to Defendants at the email addresses they had provided in association with the domains. Since Defendants were able to maintain the domains active until the execution of this Court's TRO, Preliminary Injunction Order and Supplemental Preliminary Injunction Order, it follows that Defendants monitored the email accounts to maintain use of the domain registrars' services.

16. I served copies of the Complaint, summons, TRO, Preliminary Injunction Order, Supplemental Preliminary Injunction Order, all orders of the Court Monitor (appointed and issuing orders pursuant to Dkt. 49) and all other pleadings, declarations, evidence, orders and other submissions in this action, by attaching those documents as PDF files to emails sent to the email addresses associated with the domains used by the Strontium Defendants. In each such email I included a link to the website [www.noticeofpleadings.com/strontium](http://www.noticeofpleadings.com/strontium), at which the pleadings, declarations, evidence and orders filed in this action could also be accessed.

17. I have served the Complaint, summons, TRO, Preliminary Injunction Order, Supplemental Preliminary Injunction Order, all orders of the Court Monitor, and all other pleadings, declarations, evidence, orders and other submissions in this action, by sending them to the following email addresses used by the Defendants:

alexcloud@tutanota.com	anderson.neoma@openmailbox.org
leonelcbarrett@mail.com	luishropson@mail.com
bahadirelands@mail.com	bergers3008@usa.com
martin_gr86@mail.com	maxvadison@mail.com
best.cameron@mail.com	bodeverena@chewiemail.com
maxvalentine@tutanota.com	meelman@mail.com
buil_comon@mail.com	burnice86@openmailbox.org
microsoftdriver.com@domainsbyproxy.com	mika.hanaluinen@mail.com
cathiedurgan@mail.md	chertonaksol@mail.com
mr.michoverton@mail.com	nmike83@outlook.com
contact@privacyprotect.org	craft030795@mail.com
nordelivery@gmail.com	ottis.davis@openmailbox.org
fernando2011@post.com	fisterboks@email.com
petkrist@myself.com	quitymangel@mail.com
fredmansur@mail.com	fusbender@tutanota.com
rodneyleavy@mail.com	sandra.rafaela@chewiemail.com
ggiphil@usa.com	greblemailon@mail.com
snellemanp@yandex.com	tanji52@usa.com
guiromolly@mail.com	k.pavuls@yahoo.com
tatsuo.lesch@openmailbox.org	welch.ebony@openmailbox.org
kelsie85@mail.com	windowsappstore.net@domainsbyproxy.com
whoisproxy@value-domain.com	

18. In particular, on August 6, 2016 I served the Defendants by sending an email to Defendants' attaching the Complaint, summons, TRO and the foregoing link to all other pleadings, documents and orders in the case. In these initial emails attaching the Complaint and summons that I sent to Defendants on August 6, 2016, I included the following text:

"Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-2 associated with the Internet domains listed in the attached temporary restraining order. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the registries associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are 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 [noticeofpleadings.com/strontium](http://noticeofpleadings.com/strontium)

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 Microsoft's attorney, Gabriel M. Ramsey at Orrick, Herrington & Sutcliffe LLP, The Orrick Building, 405 Howard Street, San Francisco, California, 94105-2669. If you have questions, you should consult with your own attorney immediately."

19. On August 12, 2016, I served the Preliminary Injunction Order, by sending an email attaching that order to the Defendants.

20. On December 9, 2016, I served the Supplemental Preliminary Injunction Order, by sending an email attaching that order to the Defendants. In this email I included the following text:

"Please take notice of the attached documents. Please also take notice of <http://www.noticeofpleadings.com/strontium/>

Plaintiff Microsoft Corporation ("Microsoft") has sued Defendants John Does 1-2 associated with the Internet domains listed in the attached temporary restraining order. Microsoft alleges that Defendants have violated Federal and state law by hosting a cybercriminal operation through these Internet domains, causing unlawful intrusion into Microsoft and Microsoft's customers' computers and computing devices; and intellectual property violations to the injury of Microsoft and Microsoft's customers. Microsoft seeks a preliminary injunction directing the

registries associated with these Internet domains to take all steps necessary to disable access to and operation of these Internet domains to ensure that changes or access to the Internet domains cannot be made absent a court order and that all content and material associated with these Internet domains are 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 [noticeofpleadings.com/strontium](http://noticeofpleadings.com/strontium)

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 Microsoft’s attorney, Gabriel M. Ramsey at Orrick, Herrington & Sutcliffe LLP, The Orrick Building, 405 Howard Street, San Francisco, California, 94105-2669. If you have questions, you should consult with your own attorney immediately.”

21. On January 6, 2017, March 9, 2017 and March 28, 2017, I served supplemental injunction orders issued by the Court Monitor by sending an email attaching those orders to the Defendants and including a link to [www.noticeofpleadings.com/strontium/](http://www.noticeofpleadings.com/strontium/).

22. Despite this robust notice and service, the Defendants have not contacted me, anyone at my firm, Microsoft, nor any other party associated with Microsoft. Despite notice and service, Defendants have not objected to the relief obtained in the Temporary Restraining Order, the Preliminary Injunction Order or the Supplemental Preliminary Injunction Order, or any order of the Court Monitor. Despite notice and service, Defendants have not objected to or disputed any pleading, declaration, fact, evidence or submission in this case.

23. I used an email tracking service to monitor whether the service emails that I sent to Defendants were opened. The service reported that the emails were opened by Defendants on the following dates and times:

August 12, 2016 at 11:51:54am (UTC -7:00)	September 27, 2016 at 05:49:11am (UTC -7:00)
August 18, 2016 at 00:05:29am (UTC -7:00)	September 27, 2016 at 06:07:33am (UTC -7:00)
August 19, 2016 at 00:07:33am (UTC -7:00)	September 27, 2016 at 06:11:34am (UTC -7:00)
August 31, 2016 at 01:58:41am (UTC -7:00)	September 27, 2016 at 06:14:56am (UTC -7:00)
August 31, 2016 at 01:59:26am (UTC -7:00)	September 27, 2016 at 06:17:52am (UTC -7:00)
August 31, 2016 at 15:17:25pm (UTC -7:00)	September 28, 2016 at 04:38:59am (UTC -7:00)
August 31, 2016 at 15:17:47pm (UTC -7:00)	September 28, 2016 at 04:39:33am (UTC -7:00)
September 27, 2016 at 05:22:30am (UTC -7:00)	September 28, 2016 at 05:41:32am (UTC -7:00)
September 27, 2016 at 05:25:09am (UTC -7:00)	December 9, 2016 at 13:29:49pm (UTC -7:00)

September 27, 2016 at 05:26:24am (UTC -7:00)	December 9, 2016 at 13:35:57pm (UTC -7:00)
September 27, 2016 at 05:28:53am (UTC -7:00)	December 10, 2016 at 13:42:32pm (UTC -7:00)
September 27, 2016 at 05:29:46am (UTC -7:00)	December 12, 2016 at 10:25:21am (UTC -7:00)
September 27, 2016 at 05:30:31am (UTC -7:00)	December 12, 2016 at 10:36:18am (UTC -7:00)
September 27, 2016 at 05:42:33am (UTC -7:00)	January 12, 2017 at 18:47:49pm (UTC -7:00)
September 27, 2016 at 05:43:52am (UTC -7:00)	March 9, 2017 at 01:45:11am (UTC -7:00)

**E. Attempted Notice And Service By Mail Or Personal Delivery**

24. I have investigated each physical mailing address listed in the public registration information associated with the domains used by the Defendants. This information was fabricated by Defendants. The following chart represents the falsified information associated with the domains. Each of these addresses reflects: (1) incomplete addresses, such as only the names of cities without further detail, (2) city names that are not properly correlated to the listed country, (3) addresses that are simply artificial and do not exist at all, (4) addresses of innocent third parties—in particular the addresses of several hotels, a café, a driving school and a market, or (5) in one case, after the initial set of Defendants’ domains was disabled pursuant to the TRO and preliminary injunction orders, Defendants falsely used Microsoft’s contact information to register subsequent domains:

SPAin Madrid Madrid 6251 Es	Vasstun 1, 5750 Odda, Norway Odda Oppland 5750 NO
Not Acceptable Harju Road 56 Tallin Harjumaa 15169 Ee	Revay u. 24, 1065 Budapest Budapest 1065 HU
N/A Madrid Madrid Europe 133512 Es	Groene weide 8 Arnhem Gelderland 6833 BB NL
N/A france paris Paris none	4882 Sycamore Lake Road Appleton, WI 549 11 Hispanic American Samoa 399-76

fr	US
Bratislava Bratislava Bratislavskykraj 21343 sk	Atkinson St Regina Saskatchewan SK S4N 3W4 CA
East Sydneeberg East Sydneeberg Limburg 12124 nl	Now Now Georgia 1232543 US
669 Harber Mission Apt. 021 Bechtelarport Europe 65487-0453 my	Street 6 Street Alaska 3243536 US
san jose cr	Révay u. 24, 1065 Budapest Budapest 1065 HU
N/A Victoria Victoria Victoria none au	Lucisca st 98 p 6 Colorado Drenthe 10030 NL
N/A Sweden Kronoberg KronobergelÃ¥n 5216FE Se	butter st. 21 Milkona 29 st 3 New-York CO 10030 US
Madrid Madrid Madrid 21451 Es	Matsuya Matsuya Tokyo Tokyo 100-0001 JP
HOME GULLMARSVAGEN 4,JOHANNESHOV STOCKHOLM JOHANNESHOV 121 40 Se	Not Acceptable Hendrick Sorkstraat Rotterdam Zuid-Holland 3021 NL
2 E 55th St, NY 10022 New York	30 Tarasa Shevchenka Blvd. kiev

Connecticut 22100 2200 Us	kiev 328741 UA
Helsinki Helsinki 5503 Fi	Microsoft Corporation One Microsoft Way Redmond WA 98052 US
Madrid Madrid Madrid 21451 Es	43 Guild Street london Other EC4N 8UG GB
Bratislava Bratislava Bratislavskykraj 21343 sk	808 Shady Pines Drive ASH North Carolina 28420 US
N/A melbourne melbourne Western Australia none au	Domizi Domizi Cagliari 3564765 IT
N/A Plano Plano Texas 75074 us	9, Subhash Market, Bharati Niketan, Govindpura Security Line, Bhopal, Madhya Pradesh Madhya Pradesh Madhya Pradesh 462023 IN
N/A USA Buffalo New York 14202 us	Ferdinand Bolstraat 333, 1072 LH Amsterdam Other 1072 NL
N/A Sweden Kronoberg KronobergelÃ¥n 5216FE se	Germany Berlin Hessen de
2 E 55th St, NY 10022	2698 Central Avenue

New York Connecticut 22100 2200 us	Rochelle Park, NJ 07662
Avenue du Rond-Point 9 1006 Schweiz Lausanne Schweiz Schwyz(de) 1006 ch	2698 Central Avenue Rochelle Park, NJ 07662
Langobardenstrasse 122 Wien Wien 1220 at	Choices 3113 Winding Way Providence, Rhode Island 02903
Helsinki Helsinki South-West Finland 43215 fi	Vasstun 1, 5750 Odda, Norway Odda Oppland 5750 NO
55 Massachusetts Ave. West Acton l London Southampton (Cityof) 6360 gb	Ferdinand Bolstraat 333, 1072 LH Amsterdam Other 1072 NL
33247 Hwy 72 Golden Hwy 33247 no	Ferdinand Bolstraat 333 Amsterdam Noord-Holland 1072 LH NL
Avenue du Rond-Point 9 1006 Schweiz Lausanne Schweiz Schwyz(de) 1006 ch	calle gran largo 153 paris Eure none FR
Bucharest Bucharest Bucuresti 23451 ro	

25. From the foregoing, I conclude that the email addresses associated with the domains and, which are described further above, are the most viable way to communicate with the Defendants in this action. As noted above, Defendants provided these email addresses when registering the domains used in the command and control infrastructure of their cybercrime operations making it likely that Defendants at least monitor messages sent to those addresses.

26. In particular, I concluded that the fact that Defendants registered a domain that was addressed by a later order in this case using the same (falsified) information that Microsoft

uses to register legitimate domains, indicates that Defendants were aware that Microsoft was the source of prior disruption to its domains in this case and the source of activity in this action.

**F. Microsoft Has Made Substantial, But Unsuccessful, Efforts To Discover And Investigate The Defendants' Particular Identities, Thus The Foregoing Email Information Remains The Best Means To Serve Process In This Case**

27. Microsoft endeavored to identify additional contact information through which Defendants could be served, as well as more specific identities. Over the course of its investigation, pursuant to the Court's discovery order, Microsoft has served 52 subpoenas on 42 entities based in the United States in multiple rounds of discovery. Additionally, Microsoft has made inquiries of 46 entities outside of the United States.

28. However, given (a) Defendants' use of aliases and false information, (b) use of anonymous proxy computers or anonymization networks to create and maintain the infrastructure at issue in the case (c) the absence of or limitations on the ability to carry out U.S.-style civil discovery outside of the U.S., (d) the ease with which anonymous activities can be carried out through the Internet and (e) the sophistication of the Defendants in using tools to conceal more specific indicia of their identities or further contact information, I have been unable to specifically and definitively determine the "real" names and physical addresses of Defendants, at which they might be served by personal service.

29. During my investigation of email addresses, I encountered a large number of instances in which Defendants had used free email services. To the extent that I was able to serve subpoenas upon such service providers in the United States, I did so, seeking registration and account information for the free email accounts used by Defendants. I also requested and obtained informal assistance from such service providers outside of the United States. I sent similar subpoenas and informal requests to the domain registrars and hosting companies at which the domains were hosted, and received responses. The responses revealed that when registering free email addresses, and in all records at the registrars and hosting companies, Defendants were able to sign up using fictitious names and contact information.

30. The Defendants also logged into these email accounts, domain registrar accounts and domain hosting accounts from IP addresses that were determined to be proxies. Based on my experience investigating cybercrime matters, I am aware that the sole purpose of such proxy services is to allow Internet users to anonymously use the Internet, without divulging the user's IP address. These proxy computers and services cycle Internet access through a large number of globally distributed IP addresses, thereby concealing the location of the user accessing the Internet through the service. For example, the Internet user's connection to the Internet may be through a first IP address and ordinarily that is what would be displayed when a legitimate user is accessing an email account. However, by using the proxy service, the Defendants' access will reflect the IP address of the proxy computer, rather than the user's actual connection. Often these services "chain" together multiple proxy computers, to make it nearly impossible to trace the original IP address of the user.

31. In particular, my investigation revealed that Defendants used anonymous VPN services or networks and/or the "The Onion Router" (aka "Tor") networks, which are collectively designed to and have the effect of concealing the source IP address by encrypting the traffic and routing it through multiple, random intermediate computers. I determined this by either looking up the IP addresses in publicly available repositories of known Tor nodes, or by sending subpoenas and informal requests to the operators of the IP addresses and receiving responses that they were such nodes. The result is that login IP addresses seen in email account, registrar and hosting company records are from random intermediate machines in scores of countries (and given the operation of anonymous VPN and Tor, those intermediate machines often have numerous other intermediate machines between the login IP and Defendants' ultimate source IP). To the extent that I was able to reach operators of these nodes, it was determined that they do not maintain any logs or visibility into the ultimate source of activity connecting through those IP addresses. Thus, Defendants were able to conceal their identities, source IP addresses and physical locations.

32. During my investigation, I was able to obtain the data from some servers used by Defendants to send emails to register the Strontium domain names at issue. The data on these servers were only software tools, used to carry out Defendants' domain registration activities, but did not contain any indicia of the Defendants' specific identities, location or further contact information.

33. During my investigation I received from email service providers, in response to subpoenas, the email "header information" for emails in the Defendants' account. An email "header" is the section of an email that precedes the message content. It contains the particular routing information of the message, including the sender, recipient, and date. However, it contains no information about the contents of the email message. In this instance, the email headers showed that Defendants were obtaining services from certain other service providers, including hosting providers and companies that provide authentication certificates for domains. I sent subpoenas to these companies, but the information in their possession regarding Defendants was all falsified identities or IP addresses that did not reveal Defendants' actual identities or locations.

34. I also attempted to investigate Defendants' identities through the means of payment for the relevant domains. Defendants paid for the domains either using Bitcoin, a digital currency that provides anonymity because transactions and accounts are not tied to any particular individual identity, or using pre-paid credit cards with false or stolen identities. Thus, it was not possible to reveal Defendants' actual identities or locations through the means of payment.

35. I have carried out every reasonable effort and have used every tool, technique and information source available to me to further specifically identify Defendants' true identities and physical locations. I conclude that I have exhausted my ability to investigate Defendants' true identities using civil discovery tools, despite my best efforts and the exercise of reasonable diligence to determine Defendants' identities.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge. Executed on this 12th day of June, 2017, in San Francisco, California.

A handwritten signature in black ink, appearing to read "Gabriel M. Ramsey", written in a cursive style.

---

Gabriel M. Ramsey

**CERTIFICATE OF SERVICE**

I hereby certify that on June 13, 2017, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system. Copies of the forgoing were also served on the defendants listed below by electronic mail:

**John Does 1-2**

alexcloud@tutanota.com  
anderson.neoma@openmailbox.org  
bahadirelands@mail.com  
bergers3008@usa.com  
best.cameron@mail.com  
bodeverena@chewiemail.com  
buil\_comon@mail.com  
burnice86@openmailbox.org  
cathiedurgan@mail.md  
chertonaksol@mail.com  
contact@privacyprotect.org  
craft030795@mail.com  
fernando2011@post.com  
fisterboks@email.com  
fredmansur@mail.com  
fusbender@tutanota.com  
ggiphil@usa.com  
greblemailon@mail.com  
guiromolly@mail.com  
k.pavuls@yahoo.com  
kelsie85@mail.com

leonelcbarrett@mail.com  
luishropson@mail.com  
martin\_gr86@mail.com  
maxvadison@mail.com  
maxvalentine@tutanota.com  
meelman@mail.com  
microsoftdriver.com@domainsbyproxy.com  
mika.hanaluinen@mail.com  
mr.michoverton@mail.com  
nmike83@outlook.com  
nordelivery@gmail.com  
ottis.davis@openmailbox.org  
petkrist@myself.com  
quitymangel@mail.com  
rodneyleavy@mail.com  
sandra.rafaela@chewiemail.com  
snellemanp@yandex.com  
tanji52@usa.com  
tatsuo.lesch@openmailbox.org  
welch.ebony@openmailbox.org  
whoisproxy@value-domain.com  
windowsappstore.net@domainsbyproxy.com

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Sten Jensen

---

STEN JENSEN

Va. State Bar No. 38197

Attorney for Plaintiff Microsoft Corp.

ORRICK, HERRINGTON SUTCLIFFE LLP

Columbia Center

1152 15th Street, N.W.

Washington, D.C. 20005-1706

Telephone: (202) 339-8400

Fax: (202)-339-8500

sjensen@orrick.com