The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. 15-CR-05351-RJB **MOZILLA'S MOTION TO INTERVENE OR APPEAR AS *AMICUS CURIAE* IN RELATION TO GOVERNMENT'S MOTION FOR RECONSIDERATION OF COURT'S ORDER ON THE THIRD MOTION TO COMPEL** **NOTE ON MOTION CALENDAR: Wednesday, May 11, 2016**

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

I. INTRODUCTION

On February 17, 2016, this Court entered an order granting Defendant's Third Motion to Compel. *See* Dkt. 161. Among other things, this Order required the Government to produce evidence related to a security vulnerability that it exploited in the Tor Browser. Specifically, the Government was ordered to produce the entire code it used to deploy a Network Investigative Technique that could be used to remotely place instructions on an individual's system to send back specified information. The Government has a pending Motion for Reconsideration and For Leave to Submit Filing Ex Parte and In Camera in relation to this Order. *See* Dkt 165.

Mozilla now seeks to intervene in relation to the Government's pending Motion to request modification of the Order, or in the alternative, to participate in the development of this issue as *amicus curiae* in favor of neither party, for the purpose of requesting that the Court modify its Order to require the government to disclose the vulnerability to Mozilla prior to disclosing it to the Defendant. Absent great care, the security of millions of individuals using Mozilla's Firefox Internet browser could be put at risk by a premature disclosure of this vulnerability. This risk could impact other products as well. Firefox is released under an open source license. This means that as Firefox source code is continuously developed, it is publicly available for developers to view, modify, share, and reuse to make other products, like the Tor Browser. The Tor Browser comprises a version of Firefox with some minor modifications to add additional privacy features, plus the Tor proxy software that makes the browser's Internet connection more anonymous.

Mozilla has reason to believe that the exploit that was part of the complete NIT code that this Court ordered the Government to disclose to the defense involves a previously unknown and potentially still active vulnerability in its Firefox code base. This belief rests on the fact that (1) the Tor Browser at issue relies on a modified version of the Firefox browser; (2) a prior exploit of the Tor Browser software by the government allegedly took advantage of

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

a vulnerability in Firefox code base[1]; and (3) technical experts in this case have suggested that the government has access to a Firefox vulnerability.[2] Mozilla has contacted the Government about this matter but the Government recently refused to provide any information regarding the vulnerability used, including whether it affects Mozilla's products. Accordingly, Mozilla requests that the Court modify its order to take into account how such disclosure may affect Mozilla and the safety of the several hundred million users who rely on Firefox.

If the disclosure involves a vulnerability in a Mozilla product, due process requires this Court to consider Mozilla's interests and the potentially serious public impact of any disclosure of the vulnerability before ordering the Government to make such disclosure solely to Defendant Jay Michaud ("Defendant"). "For more than a century the central meaning of procedural due process has been clear: 'Parties whose rights are to be affected are entitled to be heard.'" *Fuentes v. Shevin*, 407 U.S. 67, 80 (1972). Although Mozilla is not opposed to disclosure to the Defendant, any disclosure without advance notice to Mozilla will inevitably increase the likelihood the exploit will become public before Mozilla can fix any associated Firefox vulnerability. Public disclosure is even more likely where, as here, the protective order does not prevent knowledge about the exploit from being disclosed to third parties, but limits only the circulation of copies of the material provided by the government. The information about the exploit is likely small in quantity and easily remembered. To protect the safety of Firefox users, and the integrity of the systems and networks that rely on Firefox, Mozilla requests that the Court order that the Government disclose the exploit to Mozilla at least 14 days before any disclosure to the Defendant, so Mozilla can analyze the vulnerability, create a fix, and update its products before the vulnerability can be used to compromise the security of its users' systems by nefarious actors.[3]

---

[1] *See* Dan Goodin, *Attackers wield Firefox exploit to uncloak anonymous Tor users*, ArsTechnica http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/).

[2] Christopher Soghoian, Twitter (Apr. 28, 2016, 12:18 PM), https://twitter.com/csoghoian/status/725720824003592192.

[3] Mozilla has high confidence that it will be able to fix a vulnerability within the fourteen day period..

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main 206.757.7700 fax

II. CORPORATE DISCLOSURE STATEMENT

Mozilla Corporation states that is a wholly owned subsidiary of the Mozilla Foundation, a 501(c)(3) non-profit (collectively referred to herein as "Mozilla"). No publicly held corporation has an ownership stake of 10% or more in Mozilla.

III. STATEMENT OF INTEREST

Mozilla is a global, mission-driven organization that works with a worldwide community to create open source products like its web browser Firefox. Mozilla is guided by a set of principles that recognize, among other things, that individuals' security and privacy on the Internet are fundamental and must not be treated as optional. Mozilla seeks to intervene to protect the security of its products and the large number of people who use those products that are not a party to this proceeding The security community has publicly speculated that the software exploit that was used to deploy the NIT code ("Exploit") in the Tor Browser implicates an undisclosed vulnerability in Mozilla's Firefox web browser ("Firefox"). Firefox is among the most popular browsers in the world, with several hundred million users who rely on Firefox to discover, experience, and connect them to the internet on computers, tablets, and mobile phones.

IV. ARGUMENT

A. The Exploit Employed Here Likely Relates to a Vulnerability in the Firefox Browser.

The Government has refused to tell Mozilla whether the vulnerability at issue in this case involves a Mozilla product. Nevertheless, Mozilla has reason to believe that the Exploit the Government used is an active vulnerability in its Firefox code base that could be used to compromise users and systems running the browser. On April 13, 2016, based on the government's filings, Motherboard reported that experts believed that the FBI was aware of a vulnerability in the Firefox browser. Joseph Cox, *The FBI May Be Sitting on a Firefox Vulnerability*, Motherboard (Apr. 13, 2016).[4] The article quoted a researcher who noted that the Tor Browser at issue here "is simply Firefox running in a hardened mode." *Id.* (quoting

[4] http://motherboard.vice.com/read/the-fbi-may-be-sitting-on-a-firefox-vulnerability.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

Nicholas Weaver, *The FBI's Firefox Exploit*, Lawfare (Apr. 7, 2016)).[5] Although it is not "simple," it is true that the Tor Browser uses several million lines of code from Firefox. Further, the Government's efforts to resist disclosure here have led commentators to believe that the vulnerability has not been patched and is still effective. *Id.*; Weaver, *supra* ("The[ ] mere fact they are expending energy to do [this] may indicate the exploit is a zero day; if it were already publically known there would be limited strategic value in keeping it secret.") Use of a Firefox vulnerability to investigate Tor users would not be surprising. In 2013, the Guardian published a presentation from the NSA stating that it sought a "native Firefox exploit" to target Tor users effectively. Cox, *supra* (referencing '*Peeling back the layers of Tor with EgotisticalGiraffe*'—*read the document*, The Guardian (Oct. 4, 2013)).[6]

The parties' affidavits and documents likewise provide a reasonable basis for this belief. Special Agent Alfin stated that the NIT is a single component—a single computer instruction delivered to a defendant's computer. (Decl. of FBI Special Agent Daniel Alfin in supp. of Mot. for Reconsideration ("Alfin Dec."), Dkt. 166-2 ¶4). It is an "exploit" that took advantage of a "software vulnerability." (Dkt 166-2 ¶ 6). As such, the exploit is not malware or a program, but a command sent to exploit a vulnerability in the software used by the Defendant. The Defendant used the Tor Browser, and the Tor Browser is based on Mozilla's Firefox code. (Dkt 48-1, Aff. in supp. of Search Warrant, ¶ 7).[7] In other words, the Exploit took advantage of a vulnerability in the browser software used by the Defendant to deploy the NIT on the Defendant's computer.

Thus, caught between a wall of silence from the government, serious public speculation about potential vulnerabilities in Firefox, and evidence in the record that supports the belief that Firefox vulnerabilities are involved, Mozilla petitions the Court because the interests of its users are not adequately represented by the parties to this case.

[5] https://www.lawfareblog.com/fbis-firefox-exploit.
[6] http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.
[7] https://www.torproject.org/projects/torbrowser.html.en

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main · 206 757 7700 fax

B. The Court Should Allow Mozilla to Intervene in This Case.

Mozilla has a legitimate interest in these proceedings. Courts have long recognized the ability of "corporations and business entities" to intervene in criminal proceedings "to protect privileged or confidential information or documents obtained, or property seized, during a criminal investigation." *Harrelson v. United States*, 967 F. Supp. 909, 912-13 (W.D. Tex. 1997) (collecting cases); *see also United States v. Cuthbertson*, 651 F.2d 189, 193 (3d Cir. 1981), *cert. denied*, 454 U.S. 1056 (1981), (holding the persons affected by the disclosure of allegedly privileged materials may intervene in pending criminal proceedings and seek protective orders); *United States v. Feeney*, 641 F.2d 821, 824 (10th Cir. 1981) (holding that a party affected by disclosure of allegedly privileged materials could intervene in a criminal action to seek a protective order). Intervention in a criminal case is appropriate and permitted even though the Federal Rules of Criminal Procedure do not specifically provide for intervention. *United States v. Collyard*, CRIM. 12-0058 SRN, 2013 WL 1346202, at *2 (D. Minn. Apr. 3, 2013) ("Despite a lack of authority in the criminal rules, motions to intervene in criminal proceedings have been granted in limited circumstances where 'a third party's constitutional or other federal rights are implicated by the resolution of a particular motion, request, or other issue during the course of a criminal case.'") (quoting *United States v. Carmichael*, 342 F.Supp.2d 1070, 1072 (M.D. Ala. 2004)); *United States v. Crawford Enterprises, Inc.*, 735 F.2d 174, 176 (5th Cir. 1984) (remanding for further consideration after denial of motion to intervene where intervenor made showing it was entitled to intervention in part because it was being adversely affected by the disclosure of certain documents).

Here, intervention is warranted for reasons similar to those presented by follow-on litigation in *United States v. Swartz*, 945 F.Supp.2d 216 (D. Mass. 2013). There, after the tragic death of Mr. Swartz, the Massachusetts Institute of Technology (MIT) and JSTOR moved to intervene to partially oppose the modification of a protective order allowing the public disclosure of discovery materials containing sensitive information about vulnerabilities in the organizations' networks (among other information), without first allowing a pre-

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main · 206 757 7700 fax

production review. *Id.* at 218. Noting that "[s]everal courts have recognized this kind of limited intervention as a proper device by which third parties may assert their interest in protecting confidential materials obtained during criminal proceedings," the court permitted the organizations to intervene. *Id.* at 218-219. The court granted the organizations' motions and allowed them to review and redact discovery materials concerning vulnerabilities in their computer networks before public disclosure. *Id.* at 219, 222. Similarly Mozilla has an interest in pre-review disclosure in this case to avoid causing potential harm to innocent Firefox users. The Court should, therefore, allow Mozilla to intervene to mitigate the risks of such disclosure.

C. Due Process Requires this Court to Consider Mozilla's Rights.

Ordering disclosure of the exploit without considering Mozilla's interests violates Mozilla's procedural and substantive due process rights under the Fifth Amendment of the United States Constitution. Due process requires courts to hear and consider arguments from parties whose property interests and rights are affected by its decisions. *Mathews v. Eldridge*, 424 U.S. 319, 348 (1976). Parties "whose property interests are at stake are entitled to 'notice and an opportunity to be heard.'" *Dusenbery v. United States*, 534 U.S. 161, 167 (2002).

To consider the weight of Mozilla's interests, this Court must determine whether the Exploit to be disclosed takes advantage of an unfixed Firefox vulnerability. If it does, Mozilla will suffer harm if the Court orders the government to disclose the vulnerability to the Defendant under the existing protective order. Likewise, Mozilla continues to suffer harm by the Government's refusal to confirm at this point whether Firefox is the target of the vulnerability. "The fundamental requirement of due process is the opportunity to be heard 'at a meaningful time and in a meaningful manner.'" *Mathews*, 424 U.S. at 333; *Application of United States for Order Authorizing Installation of Pen Register or Touch-Tone Decoder and Terminating Trap*, 610 F.2d 1148, 1157 (3d Cir. 1979) (same). Due process compels this Court to hear Mozilla's arguments and consider its interests before rendering a decision.[8]

[8] "The Court's view has been that as long as a property deprivation is not *de minimis*, its gravity is irrelevant to the question whether account must be taken of the Due Process Clause." *Goss v. Lopez*, 419 U.S. 565, 576 (1975).

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206.757 7700 fax

Other courts have rejected, or altered, the relief requested by the Government to avoid placing an undue burden on affected parties. Consideration of the effect of an order on a company's products has been a frequent source of litigation under the All Writs Act. In *Application of U. S. of Am. for Or. Authorizing Installation of Pen Register or Touch-Tone Decoder and Terminating Trap*, 610 F.2d 1148, 1156 (3d Cir. 1979), the court found a deprivation of a property interest where a tracing order denied appellants the free use of their equipment and the services of their employees. *Id.* at 1156 ("The procedural guarantees of due process attach when the state deprives a person of an interest in 'liberty' or 'property'" and "[t]he most important requirement of due process is the opportunity to be heard at a meaningful time."); *see also In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865, at *2 (S.D.N.Y. Oct. 31, 2014) ("Courts have held that due process requires that a third party subject to an order under the All Writs Act be afforded a hearing on the issue of burdensomeness prior to compelling it to provide assistance to the Government."); *see also In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Ct.*, 15-mc-01902-JO, 2015 WL 5920207, at *7 (E.D.N.Y. Oct. 9, 2015) (same).

Here, the relief each party seeks—disclosure to the Defendant or continued secrecy by the Government—will affect Mozilla's property interests in its business and software. If the Exploit takes advantage of an unfixed Firefox vulnerability, and if the defense receives the Exploit, but Mozilla does not, the vulnerability will be more likely to leak and be used by bad actors, which will harm Mozilla and its users. If the Government retains the vulnerability and does not disclose it at all, Mozilla will continue to be harmed by the nondisclosure, as the vulnerabilities in its software will remain unfixed, exposing Firefox users to potential harm.[9]

[9] It is worth noting that the Government refuses to tell Mozilla if the Exploit went through the Vulnerabilities Equities Process ("VEP"), which is an interagency process used to determine whether vulnerabilities should be disclosed to the impacted company or should be exploited in secret.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main 206.757.7700 fax

D. If Mozilla Is Not Permitted to Intervene, It Should Be Allowed to Appear as *Amicus*.

If Mozilla is not permitted to intervene to protect its interests, this Court should certainly allow Mozilla to appear as *amicus curiae*. The Court has broad discretion to permit a non-party to participate in an action as *amicus curiae*. *See, e.g., Gerritsen v. de la Madrid Hurtado*, 819 F.2d 1511, 1514 n.3 (9th Cir. 1987); *Nat. Res. Def. Council v. Evans*, 243 F. Supp.2d 1046, 1047 (N.D. Cal. 2003) (*amici* "may file briefs and may possibly participate in oral argument" in district court actions). "District courts frequently welcome amicus briefs from non-parties concerning legal issues that have potential ramifications beyond the parties directly involved or if the *amicus* has 'unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide.'" *Sonoma Falls Dev., LLC v. Nevada Gold & Casinos, Inc.*, 272 F. Supp.2d 919, 925 (N.D. Cal. 2003) (quoting *Cobell v. Norton*, 246 F. Supp.2d 59, 62 (D.D.C. 2003) (citation omitted). No special qualifications are required; an individual or entity "seeking to appear as *amicus* must merely make a showing that his participation is useful to or otherwise desirable to the court." *In re Roxford Foods Litig.*, 790 F. Supp. 987, 997 (E.D. Cal. 1991).

Because Mozilla will present a unique perspective and will represent the interests of millions of Firefox users, its participation as *amicus curiae* is particularly important. *See Liberty Res., Inc. v. Philadelphia Hous. Auth.*, 395 F. Supp.2d 206, 209 (E.D. Pa. 2005). ("Courts have found the participation of an *amicus* especially proper . . . where an issue of general public interest is at stake."). This is because the primary role of an *amicus* is "to assist the Court in reaching the right decision in a case affected with the interest of the general public." *Russell v. Bd. of Plumbing Examiners of the County of Westchester*, 74 F. Supp.2d 349, 351 (S.D.N.Y. 1999). In Liberty Resources, a case brought by a disability rights advocacy group against a public housing authority, the court granted *amicus curiae* status to another advocacy group that represented residents of public housing because the group's participation "will serve to keep the Court apprised of the interests of non-disabled Section 8 voucher recipients who may be affected by this case." 395 F. Supp.2d at 209. Similarly, Mozilla here

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

will represent the interests of Firefox users in maintaining the security of the browser, an interest that is not adequately represented by the parties to this case. Accordingly, this Court should allow Mozilla to appear as *amicus curiae* and present argument on the Government's Motion for Reconsideration.

E. If the Exploit Implicates Firefox, Failure to Disclose the Vulnerability to Mozilla Threatens to Harm Mozilla, Its Developers, and Its Users.

If the Court determines that the Exploit takes advantage of an unfixed vulnerability in Firefox, disclosure to any third parties, including the defendant, before it can be fixed may threaten the security of the devices of Firefox users.[10] And neither Mozilla nor the government would know if a third-party had received information to exploit the vulnerability until potentially wide-spread damaged had occurred. Firefox is used by individuals, businesses, and governments around the world, including by the U.S. government users and by private-sector users who work as part of the critical infrastructure. As commentators have observed, "Firefox is critical computing infrastructure. Many government computers give the user a choice between Firefox and Internet Explorer. A Firefox exploit in the wrong hands could result in millions of ransomware infections or could permit an adversary to penetrate government networks through phishing URLs, watering-hole attacks, or packet-injection attacks." *Weaver, supra*.

Web browsers are an attractive means of attacking personal and corporate computers because they are the gateway experience to the Internet. In the web browser context, a severe vulnerability is an ambiguity in code that allows a third party to tell the computer to run its code, instead of what the computer should run next. Once this happens, the third party can gain total control of the computer. For example, the third party can see what the user is doing in a different browser tab, read all data on the computer, see every action the user takes or even turn on the computer's camera or microphone to watch and listen to the user. *See, e.g.*, Nate

[10] Indeed, the government's resistance to making such disclosure appears to be premised, at least in part, on the concern that the disclosure to the defendant could lead to further disclosures, bringing about exactly the type of harm that could be averted if Mozilla were made aware of the nature of the vulnerability.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main · 206 757 7700 fax

Anderson, *Meet the men who spy on women through their webcams*, ArsTechnica (Mar. 10, 2013) (describing hackers' use of a remote access tool to spy on victims through their webcams and search their computers for personal pictures).[11] The information contained in the Declaration of Special Agent Alfin suggests that the Government exploited the very type of vulnerability that would allow third parties to obtain total control an unsuspecting user's computer.[12]

The wider the use of code, the greater the harm in refusing to disclose such a vulnerability.[13] "In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems." *Id.* at 220. Mozilla's Firefox code falls into this category. Firefox is one of the most used web browsers in the world, with an installed base of several hundreds of million people around the world. *See* Mozilla Press Center, Mozilla at a Glance.[14] And even more products, like the Tor Browser, have incorporated portions of Mozilla's open source code.[15]

In light of Firefox's wide, critical uses, Mozilla's internal policies reflect the care that must be given to vulnerabilities in its code. Bug reports with security vulnerabilities are flagged and assigned special access controls to restrict them to a known group of people. (Ex. A). Mozilla often holds information about these bugs confidential until it can fix the bugs and deploy the fix to users. Although Mozilla's software development work is typically

---

[11] http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/1/.

[12] Dkt 166-2, Alfin Decl. at ¶¶ 13-15, which indicates that the NIT was delivered to Michaud's computer, and then was able to obtain data from the computer itself, such as the MAC address, which would usually not be visible to the browser.

[13] Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, 220 (Dec. 12, 2013) https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[14] https://blog.mozilla.org/press/ataglance/.

[15] http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

conducted in public forums, these security processes are intentionally not publicly visible to prevent malicious actors from learning the details of the vulnerability.

F. The Protective Order Does Not Adequately Protect Mozilla or its Users.

In light of the dangers that could stem from disclosure of the Exploit, the NIT Protective Order is not adequate to protect the sensitivity of this Exploit. A court may modify a protective order in a criminal case "for good cause." Fed. R. Crim. P. 16. Good cause exists here because, in the hands of an attacker, the Exploit may provide the ability to either extract information from or gain access to a person's computer. Mozilla is concerned with the implications to its global user base should the Exploit be disclosed to the Defendant and reveal an active vulnerability in Firefox. An attacker may use this vulnerability for nefarious purposes, including to sell the information or provide access to other individuals, organizations, or governments. It makes no sense to allow the information about the vulnerability to be disclosed to an alleged criminal, but not allow it to be disclosed to Mozilla.

Because of the serious risks associated with disclosure of a vulnerability in Mozilla's widely used source code, a previously unknown vulnerability in that source code should be treated with the care given to confidential source code containing trade secrets to prevent disclosure to unauthorized parties. In *Telebuyer, LLC v. Amazon.com, Inc.*, No. 13-CV-1677, 2014 WL 5804334, at *2 (W.D. Wash. July 7, 2014), this Court examined a protective order to determine if it adequately protected source code to be disclosed. The Court found that giving "counsel and experts the benefit of the doubt that they will faithfully observe the confidentiality rules to which the parties have already agreed" is not enough. *Id.* Vulnerabilities in code as widely used as Mozilla's are similar to source code because they create a "heightened risk of inadvertent disclosure." *Id.* (citing *Kelora Sys., LLC v. Target Corp.*, No. 11-cv-01584, 2011 WL 6000759, at *7 (N.D. Cal. Aug.29, 2011)). As with source code, "[i]t is very difficult for the human mind to compartmentalize and selectively suppress information once learned, no matter how well-intentioned the effort may be to do so." *In re Deutsche Bank Trust Co. Americas*, 605 F.3d 1373, 1378 (Fed. Cir. 2010) (citing *FTC v. Exxon Corp.*, 636 F.2d 1336,

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main · 206 757 7700 fax

1350 (D.C.Cir.1980)). Thus, disclosure to the Defendant without adequate advance notice to Mozilla in this case could cause great risk to the public.

Unlike the protective order Amazon proposed and the Court entered in Telebuyer, the protective order here turns copies of the NIT material over to the Defendant, but does not provide adequate safeguards.[16] For example, the protective order in Telebuyer required copies to be provided only on password-protected computers stored in a large room. Ex. B, Protective Order, Case No. 13-cv-01677 (W.D. Wash Aug. 7, 2014). It prohibits any viewer of the source code from possessing any input/output device while viewing the source code. It requires viewers to take notes only on a laptop not connected to any network and restricts internet access to another room. Viewers must sign a log stating when they viewed the source code, and all technical advisors must be identified and pre-approved before viewing the source code.

The protective order here contains no such restrictions. The relevant provisions of the protective order state that:

> 2. The United States will make available copies of discovery materials, including those filed under seal, to defense counsel to comply with the government's discovery obligations. Possession of copies of the NIT Protected Material is limited to the attorneys of record, members of the defense team employed by the Office of the Federal Defender, and Vlad Tsyrklevich, an expert retained by the defense team. (hereinafter collectively referred to as members of the defense team).
>
> 3. The attorneys of record and members of the defense team may display and review the NIT Protected Material with the Defendant. The attorneys of record and members of the defense team acknowledge that providing copies of the NIT Protected Material, or information contained therein, to the Defendant and other persons is prohibited, and agree not to duplicate or provide copies of NIT Protected Material, or information contained therein, to the Defendant and other persons.
>
> 4. The United States Attorney's Office for the Western District of Washington is similarly allowed to display and review the NIT Protected Material, or information contained therein, to lay witnesses, but is otherwise prohibited from providing copies of the NIT Protected Material, or information contained therein, to lay witnesses, i.e. nonlaw enforcement witnesses.

[16] Nor does it expressly permit disclosure to Mozilla. At the very least, the protective order should not interfere with such disclosure.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

(Dkt. 102). The protective order does not contain restrictions on disclosing knowledge learned through examining NIT Protected Material. This alone marks a serious deficiency in the Protective Order as the damaging information about the vulnerability is likely something that someone can easily remember. Rather, the Protective Order's disclosure restrictions are limited to the further distribution of the copies of information the defense receives from the government. Dkt. 102, ¶¶ 2-4, 8. Without more restrictive provisions, the protective order relies too heavily on the Defendant's representations he and his defense team will not share copies, but not on any explicit agreement that they will not share or use information learned or that they will put security safeguards in place.[17] As the Telebuyer court stated, a sufficient protective order should "restrict[] how, when, and where the information is displayed, how much can be printed, and how it is transported." *Id.* As in Telebuyer, the protective order here "does not do these things, and [a] promise of fidelity to the confidentiality rules, however sincere, is not a substitute." *Telebuyer, LLC*, 2014 WL 5804334 at *2.[18]

G. The Court Should Order Advance Disclosure of the Exploit to Mozilla

1. Advance Disclosure of Software Vulnerabilities to the Impacted Company is a Best Practice in the Security Community.

In reconsidering its prior order, the Court should be guided by established best practices of advance disclosure in software vulnerability management. These go by different names in the security community such as "Coordinated Disclosure," "Partial Disclosure," and "Responsible Disclosure." The underlying principle is that the security researcher who discovers the vulnerability notifies the affected company and allows some time for the vulnerability to be fixed before it is disclosed publicly, which may occur at security conferences, in papers, distribution lists, or through the company's own announcement.[19] This

[17] To the extent that the phrase "defense team" for purposes of the NIT incorporates the general protective order, the number of people who will be exposed to the vulnerability may be excessively broad. *See* (Dkt. 19 ¶ 2 (defining "defense team" to include attorneys of record, and investigators, paralegals, law clerks, experts and assistants for the attorneys of record)).

[18] Mozilla was not contacted by the Government regarding the development of the protective order and therefore played no role in the drafting of the order.

[19] https://www.mozilla.org/en-US/security/bug-bounty/

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

advance notification allows the company to evaluate the damage that may have already occurred, to fix the vulnerability, and to inform future responses to similar attack vectors. It also provides the affected company with an opportunity to mitigate any ongoing harm or additional potential harm that could be caused when a vulnerability is disclosed publicly and weaponized before it can be fixed. By contrast, if a vulnerability is publicly disclosed before a company is notified, criminals can quickly mount attacks using the published information, resulting in the proliferation of malware that can threaten the security of individual, corporate, and government networks (and the information stored therein). *See, e.g.*, Scott Culp, *It's Time to End Information Anarchy*, Microsoft TechNet (Oct. 2001) (describing the proliferation of worms following security researchers' publication of instructions for exploiting system vulnerabilities).[20]

Advance disclosure is a fundamental part of the 24/7 effort to stay ahead of attackers exploiting vulnerabilities. Mozilla receives vulnerability reports from security researchers, governments (U.S. and foreign), other companies, developers working with Firefox code, and even end users. Mozilla, *Firefox Bug Bounty Rewards*.[21] The timeframe to fix a vulnerability varies based on factors such as the severity of the issue, how complex the fix is, whether the reporter has a disclosure timeline, whether other systems are affected, and whether the vulnerability is being actively exploited. Particularly with a vulnerability that is being actively exploited, it is a race against time to fix the vulnerability and deploy an update to protect users from ongoing harm.

H. Advance Disclosure of Software Vulnerabilities to the Impacted Company is in the Public Interest.

Disclosure of vulnerabilities typically occurs in the context of security research, where the purpose is to find and disclose vulnerabilities to strengthen the underlying system. In a judicial proceeding, disclosing a vulnerability provides the defendant with information relevant

[20] https://web.archive.org/web/20011109045330/http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp

[21] *Available at* https://www.mozilla.org/en-US/security/bug-bounty/hall-of-fame/.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206 622 3150 main 206 757 7700 fax

to his case. Although these scenarios have different purposes, the underlying risks to disclosure are present in both situations. The same mitigation techniques to prevent harm to users should apply, irrespective of the purpose of disclosure.

Should the Court conclude that disclosure to the Defendant is appropriate, the best course of action is first to require the Government to acknowledge to the Court what products the Exploit affects. The Government should then be required to either notify the affected company (or companies) and provide time to fix the vulnerability and deploy updates to their users or to verify that this process has been done. Once completed, or at least underway, the Court could order the Government to disclose the Exploit to the Defendant. Applying this model of advance disclosure protects users when software vulnerabilities are disclosed through the court system.

V. CONCLUSION

Mozilla respectfully requests it be granted leave to intervene, or alternatively, be permitted to appear as *amicus curiae*. Mozilla likewise requests that, if the Court orders disclosure to the Defendant and the NIT uses an exploit or vulnerability in Mozilla's code, it also order the Government to provide information about the NIT to Mozilla 14 days prior to providing that information to the defense to allow Mozilla time to evaluate and fix the vulnerability. Finally, Mozilla requests that the protective order be modified to restrict dissemination and use of knowledge gained from reviewing the NIT Protected Material.

DATED this 11th day of May, 2016.

Davis Wright Tremaine LLP
Attorneys for Non-Party Mozilla

By */s/ James E. Howard*
James E. Howard, WSBA #37259
Jeffrey Coopersmith, WSBA #30954
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
Telephone: 206-622-3150
Fax: 206-757-7700
E-mail: jimhoward@dwt.com
jeffcoopersmith@dwt.com

Marc Zwillinger (*pro hac vice* to be filed)
Jacob Sommer (*pro hac vice* to be filed)
ZwillGen PLLC
1900 M St. NW, Ste. 250
Washington, DC 20036
(202) 296-3585
marc@zwillgen.com
Jake@zwillgen.com

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main 206.757.7700 fax