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

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

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

DWT 29515211v3 0050033-000393

Exhibit A

mozilla

Handling Mozilla Security Bugs

Version 1.1

IMPORTANT: Anyone who believes they have found a Mozilla-related security vulnerability can and should report it by sending email to the address security@mozilla.org.

Introduction

In order to improve the Mozilla project's approach to resolving Mozilla security vulnerabilities, mozilla.org is creating more formal arrangements for handling Mozilla security-related bugs. First, mozilla.org is appointing a security module owner charged with primary responsibility for coordinating the investigation and resolution of reported Mozilla security vulnerabilities; the security module owner will have one or more peers to assist in this task. At the same time mozilla.org is also creating a larger "Mozilla security bug group" by which Mozilla contributors and others can participate in addressing security vulnerabilities in Mozilla. This document describes how this new organizational structure will work, and how security-related Mozilla bug reports will be handled.

Note that the focus of this new structure is restricted solely to addressing actual security vulnerabilities arising from problems in Mozilla code. This work is separate from the work of developers adding new security features (cryptographically-based or otherwise) to Mozilla, although obviously many of the same people will be involved in both sets of activities.

Background

Security vulnerabilities are different from other bugs, because their consequences are potentially so severe: users' private information (including financial information) could be exposed, users' data could be destroyed, and users' systems could be used as platforms for attacks on other systems. Thus people have strong feelings about how security-related bugs are handled, and in particular about the degree to which information about such bugs is publicly disclosed.

The Mozilla project is a public software development project, and thus we have an inherent bias towards openness. In particular, we understand and acknowledge the concerns of those who believe that all information about security vulnerabilities should be publicly disclosed as soon as it is known, so that users may take immediate steps to protect themselves and so that problems can get the maximum amount of developer attention and be fixed as soon as possible.

At the same time the Mozilla project receives substantial contributions of code and developer time from organizations that use (or plan to use) Mozilla code in their own product offerings. Some of these products may be used by large populations of end users, many of whom may not often upgrade or check for recent security fixes. We understand and acknowledge the concerns of those who believe that too-hasty disclosure of exploit details can provide a short-term advantage to potential attackers, who can exploit a problem before most end users become aware of its existence.

We believe that both sets of concerns are valid, and that both are worth addressing as best we can. We have attempted to create a compromise scheme for how the Mozilla project will handle reports of security vulnerabilities. We

About Mozilla
Mission
History
Leadership
Governance
Forums
Patents

Our Products
Software and other innovations designed to advance our mission.
Learn More »

Get Involved
Become a volunteer contributor in a number of different areas.
Learn More »

believe that it is a compromise that can be justified to those on both sides of the question regarding disclosure.

General policies

mozilla.org has adopted the following general policies for handling bug reports related to security vulnerabilities:

- Security bug reports can be treated as special and handled differently than "normal" bugs. In particular, the mozilla.org Bugzilla system will allow bug reports related to security vulnerabilities to be marked as "Security-Sensitive," and will have special access control features specifically for use with such bug reports. However a security bug can revert back to being a normal bug (by having the "Security-Sensitive" flag removed), in which case the access control restrictions will no longer be in effect.
- Full information about security bugs will be restricted to a known group of people, using the Bugzilla access control restrictions described above. However that group can and will be expanded as necessary and appropriate.
- As noted above, information about security bugs can be held confidential for some period of time; there is no pre-determined limit on how long that time period might be. However this is offset by the fact that the person reporting a bug has visibility into the activities (if any) being taken to address the bug, and has the power to open the bug report for public scrutiny.

The remaining sections of the document describe in more detail how these general policies have been implemented in practice.

Organizational structure for handling security bugs

We are organizing the investigation and fixing of Mozilla security vulnerabilities similar to the way Mozilla project activities are handled in general: There will be a security module owner, a small core group of active contributors who can act as peers to the module owner, a larger group of less active participants, and other people who may become involved from time to time. As with other parts of the Mozilla project, participation in Mozilla security-related activities will be open to both independent volunteers and to employees of the various corporations and other organizations involved with Mozilla.

The Mozilla security module owner and peers

The Mozilla security module owner will have a similar level of power and responsibility as other Mozilla module owners; also as with other Mozilla module owners, mozilla.org staff will oversee the work of the security module owner and select a new security module owner should that ever be necessary for any reason.

The Mozilla security module owner will work with mozilla.org staff to select one or more people to act as peers to the security module owner in investigating and resolving security vulnerabilities; the peers will share responsibility for overseeing and coordinating any and all activities related to security bugs.

The Mozilla security bug group

The Mozilla security module owner and peers will form the core of the Mozilla security bug group, and will select a number of other people to round out the group's membership. Each and every member of the Mozilla security bug group will automatically have access to all Mozilla bugs marked "Security-Sensitive." The members of the Mozilla security bug group will be drawn primarily from the following groups:

- security developers (i.e., those whose bugs are often singled out as security-relevant or who have security-relevant bugs assigned to them), and security QA

people who are the QA contacts for those bugs;
- "exploit hunters" with a good track record of finding significant Mozilla security vulnerabilities;
- representatives of the various companies and groups actively distributing Mozilla-based products; and
- super-reviewers and drivers.

(The Bugzilla administrators will technically be in the Mozilla security bug group as well, mainly because they already have visibility into all Bugzilla data hosted through mozilla.org.)

The Mozilla security bug group will have a private mailing list, security-group@mozilla.org, to which everyone in the security bug group will be subscribed. This list will act as a forum for discussing group policy and the addition of new members, as described below. In addition, Mozilla.org will maintain a second well-known address, security@mozilla.org, through which people not on the security group can submit reports of security bugs. Mail sent to this address will go to the security module owner and peers, who will be responsible for posting the information received to Bugzilla, and marking the bug as "Security-Sensitive" if it is warranted given the nature and severity of the bug and the risk of potential exploits.

Other participants

Besides the permanent security bug group members described above, there are two other categories of people who may participate in security bug group activities and have access to otherwise-confidential security bug reports:

- A person who reports a security bug will have continued access to all Bugzilla activities associated with that bug, even if the bug is marked "Security-Sensitive."
- Any other persons may be given access to a particular security bug, by someone else (who does have access) adding them to the CC list for that bug.

Thus someone reporting a security bug in essence becomes a member of the overall group of people working to investigate and fix that particular vulnerability, and anyone else may be easily invited to assist as well if and when that makes sense.

Expanding the Mozilla security bug group

As previously described, the Mozilla security module owner can select one or more peers to share the core work of coordinating investigation and resolution of Mozilla security vulnerabilities, and will work with them to create some agreed-upon ground rules for how this work can be most effectively shared among themselves. As with other Mozilla modules, we intend that this core group (module owner plus peers) remain small; its membership should change only infrequently and only after consultation with mozilla.org staff.

The security module owner and peers will also work with mozilla.org to populate the initial security bug group. We expect that the Mozilla security bug group will initially be significantly larger than the core group of module owner and peers, and that it may grow even further over time. New members can be added to the Mozilla security bug group as follows:

- New people can apply to join the security bug group, or may be recruited by existing members. Applicants for membership must have someone currently in the security bug group who is willing to vouch for them and nominate them for membership. Nomination is done by the "voucher" sending email to the security bug group private mailing list.
- The applicant's nomination for membership will then be considered for a period of a few days, during which members of the security bug group can speak out in favor of or against the applicant.

- At the end of this period, the security module owner will decide to accept the applicant or not, based on feedback and objections from the security bug group in general and from the module owner's peers in particular. If anyone else in the security bug group has a problem with the module owner's decision then they can appeal to mozilla.org staff, who will make the final decision.

The criteria for membership in the Mozilla security bug group are as follows:

- The applicant must be trusted by those already in the group.
- The applicant should have a legitimate purpose for wishing to join the group.
- The applicant must be able to add value to the group's activities in some way.

In practice, if over time a particular person happens to be frequently added to the CC list for security-sensitive bugs then they would be a good candidate to be invited to join the security bug group. (As described previously, once added to the security bug group that person would then have automatic access to all bugs marked security-sensitive, without having to be explicitly added to the CC list for each one.)

Note that although we intend to make it relatively simple for a new person to join the security bug group, and we are not limiting the size of the group to any arbitrary number, we also don't want the group to expand without any limits whatsoever. We reserve the right to cap the membership at some reasonable level, either by refusing new applications or (if necessary and appropriate) by removing some existing members of the security bug group to make room for new ones.

Disclosure of security vulnerabilities

The security module owner, peers, and other members of the Mozilla security bug group will *not* be asked to sign formal nondisclosure agreements or other legal paperwork. However we do expect members of the group

- not to disclose security bug information to others who are not members of the Mozilla security bug group or are not otherwise involved in resolving the bug, except that if a member of the Mozilla security bug group is employed by a distributor of Mozilla-based products, then that member may share such information within that distributor, provided that this information is shared only with those who have a need to know, only to the extent they need to know, and such information is labeled and treated as the organization generally treats confidential material,
- not to post descriptions of exploits in public forums like newsgroups, and
- to be careful in whom they add to the CC field of a bug (since all those CC'd on a security bug potentially have access to the complete bug report).

When a bug is put into the security bug group, the group members, bug reporter, and others associated with the bug will decide by consensus, either through comments on the bug or the group mailing list, whether an immediate warning to users is appropriate and how it should be worded. The goals of this warning are:

- to inform Mozilla users and testers of potential security risks in the versions they are using, and what can be done to mitigate those risks, and
- to establish, for each bug, the amount of information a distributor can reveal immediately (before a fix is available) without putting other distributors and their customers at risk.

A typical warning will mention the application or module affected, the affected versions, and a workaround (e.g. disabling JavaScript). If the group decides to publish a warning, the module owner, a peer, or some other person they may designate will post this message to the Known Vulnerabilities page (which will be the authoritative source for this information) and will also send a copy of this message to an appropriate moderated mailing list and/or newsgroup (e.g., netscape.public.mozilla.announce and/or some other newsgroup/list established

specifically for this purpose). Mozilla distributors who wish to inform their users of the existence of a vulnerability may repost any information from the Known Vulnerabilities page to their own websites, mailing lists, release notes, etc., but should not disclose any additional information about the bug.

The original reporter of a security bug may decide when that bug report will be made public; disclosure is done by clearing the bug's "Security-Sensitive" flag, after which the bug will revert to being an ordinary bug. We believe that investing this power in the bug reporter simply acknowledges reality: Nothing prevents the person reporting a security bug from publicizing information about the bug by posting it to channels outside the context of the Mozilla project. By not doing so, and by instead choosing to report bugs through the standard Bugzilla processes, the bug reporter is doing a positive service to the Mozilla project; thus it makes sense that the bug reporter should be able to decide when the relevant Bugzilla data should be made public.

However we will ask all individuals and organizations reporting security bugs through Bugzilla to follow the voluntary guidelines below:

- Before making a security bug world-readable, please provide a few days notice to the Mozilla security bug group by sending email to the private security bug group mailing list.
- Please try not to keep bugs in the security-sensitive category for an unreasonably long amount of time.
- Please try to be understanding and accommodating if a Mozilla distributor has a legitimate need to keep a bug in the security-sensitive category for some reasonable additional time period, e.g., to get a new release distributed to users. (Regarding this point, if all Mozilla distributors have a representative on the security bug group, then even if a bug remains in the security-sensitive category all affected distributors can still be informed and take appropriate action.)

The security module owner will be the primary person responsible for ensuring that security bug reports are investigated and publicly disclosed in a timely manner, and that such bug reports do not remain in the Bugzilla database uninvestigated and/or undisclosed. If disputes arise about whether or when to disclose information about a security bug, the security bug group will discuss the issue via its mailing list and attempt to reach consensus. If necessary mozilla.org staff will serve as the "court of last resort."

A final point about duplicate bug reports: Note that security bugs marked as duplicates are still considered separate as far as disclosure is concerned. Thus, for example, if a particular security vulnerability is reported initially and then is independently reported again by someone else, each bug reporter retains control over whether to publicly disclose their own bug, but their decision will not affect disclosure for the bug reported by the other person.

Changing this policy

This policy is not set in stone. It is our hope that any disputes that arise over membership, disclosure, or any other issue addressed by this policy can be resolved by consensus among the Mozilla security module owner, the module owner's peers, and other security bug group members through discussions on the private security bug group mailing list.

As with other Mozilla project issues, mozilla.org staff will have the final authority to make changes to this policy, and will do so only after consulting with the various parties involved and with the public Mozilla community, in order to ensure that all views are taken into account.

Exhibit B

The Honorable Barbara J. Rothstein

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

TELEBUYER, LLC, Plaintiff, v. AMAZON.COM, INC., AMAZON WEB SERVICES LLC, and VADATA, INC., Defendants.	Case No. 2:13-cv-01677-BJR [redacted] **PROTECTIVE ORDER**
AMAZON.COM, INC., AMAZON WEB SERVICES LLC, and VADATA, INC., Counterclaimants, v. TELEBUYER, LLC, Counterclaim-Defendant.	

Plaintiff Telebuyer, LLC. ("Telebuyer") and defendants Amazon.com, Inc., Amazon Web Services LLC, and VADATA, Inc. (collectively "Amazon") anticipate that documents, testimony, or information containing or reflecting confidential, proprietary, trade secret, and/or commercially sensitive information are likely to be disclosed or produced during the course of discovery in this litigation and request that the Court enter this Order setting forth the conditions for handling, treating, obtaining, and using such information.

Pursuant to Rule 26(c) of the Federal Rules of Civil Procedure, the Court finds good cause for entry of the following Protective Order ("Order" or "Protective Order").

I. PROTECTED CONFIDENTIAL INFORMATION

Discovery materials produced in this case may be labeled as one of three categories: CONFIDENTIAL, CONFIDENTIAL OUTSIDE COUNSEL ONLY and RESTRICTED CONFIDENTIAL – SOURCE CODE, as set forth in subsections A through C below. All three of the identified categories of information are referred to collectively in this Order as "Protected Information." Each party or nonparty that designates material for protection under this Protective Order shall limit any such designation to only that material, or parts of material, that qualify for the designation assigned to that material. No party or nonparty shall utilize any mass, indiscriminate, or routinized designations for protection under this Order.

A. Information Designated as "Confidential Information"

1. For purposes of this Order, "CONFIDENTIAL INFORMATION" shall mean all information or material produced for or disclosed in connection with this action to a receiving party that a producing party, including any party to this action and any non-party producing information or material voluntarily or pursuant to a subpoena or a court order in connection with this action, considers in good faith to constitute confidential technical, sales, marketing, financial, or other commercially sensitive information, whether embodied in physical objects, documents, or the factual knowledge of persons, and which has been so designated by the producing party. "CONFIDENTIAL INFORMATION" shall include, for example, the following documents and tangible things produced or otherwise exchanged: non-public technical documents

and things pertaining to the design, test, development, architecture, and operation of the accused systems/processes, including schematics, drawings, flow charts, specifications, source code, pseudocode, source code documentation, and other design documents; financial records and/or related documents; communications pertaining to the revenue and profits of the accused systems/processes; documents and communications containing information or data relating to future products not yet commercially released; documents and communications containing information or data relating to business, marketing, and/or product strategy; documents and communications containing information or data relating to commercial or settlement agreements; documents and communications relating to market and/or competitive analyses; third-party confidential information, etc.

2. The following information is not CONFIDENTIAL INFORMATION:

a. Any information that is or, after its disclosure to a receiving party, becomes part of the public domain as a result of act(s) not involving a violation of this Order, including but not limited to becoming a part of the public record through trial or otherwise;

b. Any information that was already publicly known or obtainable prior to the disclosure; and,

c. Any information that was received by the receiving party from a source who obtained the information lawfully and under no obligation of confidentiality to the producing party.

3. Unless otherwise ordered by the Court or agreed to by the producing party, documents, information or other material designated as containing CONFIDENTIAL INFORMATION and information contained therein shall be made available only to:

a. Outside litigation counsel of record and supporting personnel employed in the law firm(s) of outside litigation counsel of record, such as attorneys, paralegals, legal translators, financial and technical analysts, IT staff, litigation support staff, legal secretaries, legal clerks, filing room staff and shorthand reporters;

b. Technical advisers and their necessary support personnel, subject to

the provisions of paragraphs I.F.1 through I.F.7 herein, provided that such disclosure(s) are only to the extent necessary, and further provided that: (a) such technical adviser(s) have signed the acknowledgement form attached hereto as Attachment A agreeing to be bound by the terms of this Order, and (b) there are no unresolved objections to such disclosure(s) existing after proper notice has been given to all parties as set forth in this Protective Order; the term "technical adviser" shall mean independent outside expert witnesses or consultants (i.e., not employees of a party) with whom counsel may deem it necessary to consult;

c. One in-house counsel designated by each party with responsibility for managing this litigation;

d. The Court, its personnel and stenographic reporters (upon such terms as the Court deems proper), as well as any court considering any appeal or petition in this matter and that court's personnel;

e. Independent legal translators retained to translate in connection with this action; independent stenographic reporters and videographers retained to record and transcribe testimony in connection with this action; graphics, translation, or design services retained by counsel for purposes of preparing demonstratives or other exhibits for deposition, trial, or other court proceedings in the actions; prior art search firms; non–technical jury or trial consulting services, including mock jurors, who have signed the form attached hereto as Attachment A;

f. Litigation support vendors specifically retained to assist outside counsel of record with document collection, production, review, and duplication services;

g. Witnesses who have been subpoenaed or noticed to testify and/or do testify at a deposition, hearing or trial in this Action subject to the limitations set forth in Paragraph I.H.2; and,

h. Any mediator or arbitrator chosen by the parties or designated by the Court regarding this matter.

B. Information Designated "Confidential Outside Counsel Only"

1. The CONFIDENTIAL OUTSIDE COUNSEL ONLY designation is

reserved for extremely sensitive CONFIDENTIAL INFORMATION that constitutes or contains (a) trade secrets or commercially sensitive competitive information, including, without limitation, information obtained from a nonparty pursuant to a current Nondisclosure Agreement ("NDA"); (b) information or data relating to future products not yet commercially released and/or strategic plans pertaining to future products, including, but not limited to: nonpublic technical information, including schematic diagrams, technical reference manuals, and operations manuals; and, (c) commercial agreements, settlement agreements or settlement communications, the disclosure of which is likely to cause harm to the competitive position of the producing party. In determining whether information should be designated as CONFIDENTIAL OUTSIDE COUNSEL ONLY, each party agrees to use such designation only that party believes in good faith that the information must be protected from disclosure to the Parties themselves (and to any Non-Party) in this litigation.

2. Documents, information, or other material designated CONFIDENTIAL OUTSIDE COUNSEL ONLY and information contained therein shall be made available only to the persons or entities listed in paragraphs I.A.3.a, b, d, e, f, g, and h, and subject to any terms set forth or incorporated therein.

C. Information Designated Restricted Confidential – Source Code

1. The "RESTRICTED CONFIDENTIAL – SOURCE CODE" designation shall be limited to extremely sensitive items representing computer code and associated comments and revision histories, formulas, engineering specifications, or schematics that define or otherwise describe in detail the algorithms or structure of software or hardware designs, disclosure of which to another party or non-party would create a substantial risk of serious harm that could not be avoided by less restrictive means. The following conditions shall govern the production, review and use of Protected Information designated as "RESTRICTED CONFIDENTIAL – SOURCE CODE" ("Source Code").

2. All Source Code shall be subject to the following provisions:

a. Unless otherwise agreed upon by the producing and receiving

parties, the Source Code shall be made available in electronic format on one or more password protected computers ("secured computers") in a locked room ("Source Code reviewing room") large enough to accommodate at least three individuals at one of the following locations: (1) a California office of the producing party's outside counsel of record in this action, or (2) a location mutually agreed upon by the receiving and producing parties. For purposes of this Order, multiple, related defendants may together constitute a single producing party if they are jointly producing Source Code for inspection.

b. Use or possession by any of the parties' representatives and technical advisers of any input/output device (e.g., USB memory stick, cameras, CDs, floppy disk, portable hard drive, etc.) is prohibited while accessing computers containing the Source Code. The parties' representatives and technical advisers shall be permitted to use personal cellular telephones in order to consult with one another or outside counsel, but may not use the camera function of cellular telephones within the Source Code reviewing room.

c. The parties' representatives and technical advisers shall be entitled to take notes relating to the Source Code electronically on a laptop that is not connected to any wired or wireless network, but may not use the laptop to capture images or copy sections of the Source Code. Each party's outside counsel and approved technical advisers shall maintain any such notes as "CONFIDENTIAL OUTSIDE COUNSEL ONLY." Internet access will be provided in a room adjacent to the Source Code reviewing room.

d. All persons entering the locked room containing the Source Code must agree to submit to reasonable security measures to insure they are not carrying any prohibited items before they will be given access to the locked room.

e. The computers containing Source Code will be made available for inspection with 24 hours' notice during regular business hours, which for purposes of this provision shall be 8:00 a.m. through 6:00 p.m., Monday through Friday, local time at the Source Code reviewing room, and other days and/or times agreed upon by the receiving and producing parties. Upon reasonable notice from the receiving party, the producing party shall make

reasonable efforts to accommodate the receiving party's request for access to the secured computer(s) outside of normal business hours. For purposes of this provision, three (3) business days is reasonable notice.

f. The producing party shall make all relevant and properly requested Source Code available electronically and in text searchable form in its native format and in a file structure that mirrors the file structure of the Source Code as maintained by the producing party when this Action was filed.

g. To the extent necessary, the producing party shall provide the receiving party with information explaining how to access the Source Code on the computers.

h. Each secured computer shall be provided with software allowing for efficient searching and review of the Source Code. In addition, the receiving party's outside counsel and/or technical advisers may request that commercially available licensed software tools for viewing and searching Source Code be installed on the secured computers provided, however, that (a) the receiving party possesses any appropriate license to such software tools; (b) the tools are in compliance with all of the terms, conditions and protections herein; and, (c) the producing party approves such software tools (such approval shall not be unreasonably withheld). If the producing party is not in possession of the requested software tools, the receiving party must provide the producing party with the CD or DVD containing such software tool(s) at least three business days in advance of the inspection, and any such CDs or DVDs will be returned to the receiving party after the producing party has loaded the software tools on the secured computers.

i. No person shall copy, e-mail, transmit, upload, download, print, photograph, or otherwise duplicate any portion of the designated Source Code, except as provided in this Order. The receiving party may print or request portions of Source Code to be printed by the producing party, but only to the extent the receiving party deems it reasonably necessary for use in this action. The receiving party shall not print Source Code in order to review or analyze blocks of Source Code elsewhere in the first instance, i.e., as an alternative to reviewing the Source Code electronically on secured computers, as the parties acknowledge and agree that the purpose

of the protections herein would be frustrated by printing portions of code for review and analysis elsewhere. Each secured computer shall be equipped with a printer to print copies of the Source Code on paper provided by the producing party, which may be watermarked, colored, and/or pre-Bates numbered. Under no circumstances are original printouts of the Source Code to be made except directly onto paper provided by the producing party. The secured computers will be programmed to print on each page a header that identifies the full pathname or other identifying information of the section of Source Code being printed, as well as line numbers of printed Source Code, provided that the inspection software tools do not impede the producing party's ability to print such headers and line numbers. Counsel for the producing party will keep the original printouts, and, absent a dispute as to the reasonableness of the printing request, shall provide copies of such original printouts to counsel for the receiving party within two (2) business days of being notified that such original printouts have been made. No copies of all or any portion of the Source Code may leave the room in which the Source Code is inspected except as provided herein. Except as otherwise provided herein, the receiving party shall not request printing of any continuous block of Source Code that results in more than twenty-five (25) printed pages, unless it is reasonably required for printing a source code function or method in its entirety. The receiving party shall not request printing of more than fifteen hundred (1500) pages in aggregate per producing party during the case. If the receiving party wishes to exceed the twenty-five (25) continuous page limit and/or the fifteen hundred (1500) aggregate limit, the receiving party may request a meet and confer to discuss the printing of additional code. If no resolution can be reached, the receiving party shall be entitled to seek a Court resolution permitting additional print requests.

j. Any printed pages of Source Code may not be copied, digitally imaged or otherwise duplicated, including, without limitation, copying, removing, or transferring the Source Code onto any other computers or peripheral equipment except: (a) by outside counsel for the receiving party for the sole purpose of creating hard duplicate copies for retention in the offices of persons authorized to access and review the source code as specified by subparagraphs l

and n; and (b) as necessary for printing exhibits (up to three (3) copies) used at depositions, expert reports, court filings, mediation or arbitration briefs, or exhibits used at trial or court hearings as discussed below. With respect to provision (a), the paper copies must be kept at all times in a secured and locked room. The receiving party's outside counsel may make no more than six (6) paper copies of any page of the Source Code received for the purpose of creating hard duplicate copies for retention in multiple offices. The parties agree that additional copies made under provision (b) shall not count toward the six (6) copy limit. To the extent the receiving party seeks to make additional paper copies of a particular producing party's Source Code, the Parties shall meet and confer in good faith. Except as provided herein, the receiving party will not electronically transmit any Source Code in any way, including, but not limited to, electronic transmission from the producing party's facilities or the offices of its outside counsel of record. This provision does not prevent the parties from including Source Code information, when necessary, in discovery responses or disclosures or in e-filings to the Court made under seal. Unless otherwise agreed by the producing and receiving parties, service copies of such e-filings are to be served via secure FTP.

k. To the extent a producing party possesses any discoverable document that partially contains information that, if standing alone, would be properly designated "RESTRICTED CONFIDENTIAL – SOURCE CODE," the producing party shall to the extent reasonable 1) redact the information from that document and produce the redacted document Bates numbered and under a non-source code designation; and 2) upon request of the receiving party, produce an unredacted copy of the document on the Source Code computer or in paper form pursuant to section I.C.2.i. The parties agree to meet and confer in good faith to resolve any issues that may arise as a result of this provision. Paper copies of such documents will not count against any limit on the number of pages of Source Code that the receiving party may request.

l. Any paper copies designated "RESTRICTED CONFIDENTIAL – SOURCE CODE," whether printed by the receiving party or the producing party, shall be stored or viewed only at (i) the offices of outside counsel for the receiving party, (ii) the site where any

deposition is taken; (iii) the Court; (iv) any intermediate location necessary to transport the information to a hearing, trial, mediation, arbitration or deposition; or (v) offices of technical advisers who have been approved to access Source Code. At depositions relating to the Producing Party's source code, and upon a reasonable and timely request by the receiving party, the Producing Party will make available for use as deposition exhibits a complete set of produced paper copies of Source Code. Any Source Code transported outside of counsel's office shall be kept in the possession of an individual specified in Paragraphs I.C.n.1 and I.C.n.2, or in a secure, locked location at all times. Such Source Code may be hand-transported only by an individual specified in Paragraphs I.C.n.1 and I.C.n.2, and shall not be placed in checked luggage, mail, FedEx, or any other means of transportation.

m. The producing party may require that all individuals, upon each entry or exit of the Source Code reviewing room by that individual, sign a log, provided by the producing party, indicating the name of that individual, whether the individual entered or exited the Source Code reviewing room, and the date and time of such entry or exit. The producing party shall be entitled to have a person monitor all entrances and exits from the Source Code viewing room. The producing party shall also be entitled to visually monitor, in a non-intrusive fashion and at reasonable intervals, the receiving party's activities in the Source Code viewing room from outside such room, through a glass wall or window, so long as the producing party cannot hear the receiving party or see the contents of the receiving party's notes or the display of any secured computer(s). However, the producing party may not use a video camera or other recording device to monitor the Source Code viewing room or the activities of the receiving party, nor may the producing party physically enter the Source Code reviewing room when the receiving party is present, without the receiving party's consent. The producing party shall not monitor the review conducted by the receiving party through analyzing the electronic access record on the secured computer (e.g., command histories, recent file lists, file access dates, undo histories, and etc.) or otherwise, all of which the producing party acknowledges constitutes the receiving party's work product and shall not be used for any purpose or admitted into evidence in this or any other

proceeding. The foregoing is not intended to restrict in any way the producing party's ability or right to otherwise ensure, for example, that the Source Code remains secure and the secured computer(s) have not been tampered with, and that the provisions of the Order have not been violated.

n. Only the following individuals shall have access to "RESTRICTED CONFIDENTIAL – SOURCE CODE" materials, absent the express written consent of the producing party or further court order:

1) Outside counsel of record for the parties to this action, including any attorneys, paralegals, technology specialists and clerical employees of their respective law firms;

2) Up to four (4) technical advisers pre-approved in accordance with Paragraphs I.F.1-I.F.7;

3) The Court, its technical adviser (if one is appointed), the jury, court personnel, and court reporters or videographers recording testimony or other proceedings in this action. Court reporters and/or videographers shall not retain or be given copies of any portions of the Source Code. If used during a deposition, the deposition record will identify the exhibit by its production Bates numbers;

4) While testifying or preparing to testify at a deposition, hearing or trial in this action only: (i) any current or former officer, director or employee of the producing party or original source of the information; (ii) any person designated by the producing party to provide testimony pursuant to Rule 30(b)(6) of the Federal Rules of Civil Procedure; and/or (iii) any person who authored, previously legally received (other than in connection with this litigation), or was directly involved in creating, modifying, or editing the Source Code, as evident from its face or reasonably certain in view of other testimony or evidence. Persons authorized to view Source Code pursuant to this sub-paragraph shall not retain or be given copies of the Source Code except while so testifying.

o. A party may make and use copies and excerpts of the Source Code if

necessary for the preparation of court filings, expert reports, demonstrative exhibits, and attorney work product. All such documents shall either be clearly marked "RESTRICTED CONFIDENTIAL – SOURCE CODE" and, if filed, shall be filed under seal, or those pages containing quoted source code shall be separately bound, and marked "RESTRICTED CONFIDENTIAL – SOURCE CODE". A receiving party shall make a good faith effort to quote the minimum amount of Source Code necessary in any such document.

p. Unless agreed by the parties, excerpts or copies of Source Code shall not be included in correspondence between counsel (references to production numbers and/or file names shall be used instead).

q. Copies of Source Code that are marked as deposition exhibits shall not be provided to the Court Reporter or attached to deposition transcripts; rather, the deposition record will identify the exhibit by its production numbers.

r. The receiving party's outside counsel may only disclose a copy of the Source Code to individuals specified in Paragraph n above (e.g., Source Code may not be disclosed to in-house counsel).

s. Beginning two weeks prior to the date set for trial and continuing through the end of trial, access to the Source Code computers must be provided under the same conditions and with the same limitations and restrictions as provided in this Section, in the city where the trial has been scheduled to occur. At the receiving party's request and upon reasonable notice, the producing party shall make a Source Code computer available during depositions of the producing party's witnesses and experts.

t. Unless otherwise agreed in advance by the parties in writing, following each day on which inspection of Source Code is done under this Order, the receiving party's outside counsel and/or experts shall remove all notes, documents, and all other materials from the room that may contain work product and/or attorney-client privileged information. The producing Party shall not be responsible for any items left in the room following each inspection session. The Parties agree that any notes, documents, or items left behind in the Source Code

review room (including electronic records on the secured computers such as command histories and file access records) shall not constitute a waiver of any applicable privilege or protection in this litigation or any other proceeding. The Producing Party shall notify the receiving party of any such inadvertently left notes, documents, or items, and shall return and/or destroy such notes, documents, or items.

u. A party's agreement to the entry of this Order shall not be deemed an admission that the party must produce Source Code in this lawsuit.

D. Identifying Protected Information

1. A producing party may designate documents or written discovery responses as Protected Information by affixing a legend reading CONFIDENTIAL, CONFIDENTIAL OUTSIDE COUNSEL ONLY or RESTRICTED CONFIDENTIAL – SOURCE CODE (if printed), on each page that contains Protected Information prior to or at the time copies are furnished to the receiving party. For documents produced in native format, the producing party shall affix the appropriate legend prominently on the medium on which such documents are produced in native format.

2. For other tangible things and information designated as Protected Information, the producing party shall affix the appropriate legend prominently on any tangible thing or media not addressed in the immediately preceding paragraph or, if not feasible to affix the legend to the thing or media, on the exterior of any case or container in which the information or item is stored.

3. Any Protected Information not reduced to documentary, tangible or physical form or which cannot be conveniently designated as set forth in the two immediately preceding paragraphs, shall be designated by the producing party by informing the receiving party of the designation in writing at or before the time of the disclosure or production of the Protected Information.

4. A party or non-party offering or sponsoring testimony at a deposition or other proceeding may identify on the record, before the close of the deposition or other proceeding,

that a specific portion of the testimony contains CONFIDENTIAL, CONFIDENTIAL OUTSIDE COUNSEL ONLY, or RESTRICTED CONFIDENTIAL – SOURCE CODE material. When it is impractical to identify separately each portion of testimony that is entitled to protection, and when it appears that substantial portions of the testimony may qualify for protection, the party or non-party that offers or sponsors the testimony may invoke on the record (before conclusion of the deposition or proceeding) a right to have up to fifteen (15) days from the date of receipt of the transcript to identify the specific portions of the testimony as to which protection is sought and to specify the level of protection being asserted, or to supplement the confidentiality designations made on the record. When this right has been invoked on the record, the transcript of the deposition or proceeding shall be treated as "CONFIDENTIAL OUTSIDE COUNSEL ONLY" until the sooner of (a) receipt of the designations by the receiving party, or (b) expiration of the fifteen (15) day period. In the alternative, when it appears that substantially all of the testimony qualifies for protection, the party or non-party may designate on the record the entire testimony as CONFIDENTIAL or CONFIDENTIAL OUTSIDE COUNSEL ONLY material.

E. Use of Protected Information in Filings with the Court

1. This Order does not prospectively authorize sealing of Protected Information filed in the judicial record. The parties acknowledge that Local Civil Rule 5(g) sets forth the procedures that must be followed and the standards that will be applied when a party seeks permission from the court to file material under seal.

2. In the event a party wishes to use any Protected Information produced by another party or nonparty in any pleading or document filed with the Court in this litigation, or as an exhibit at a hearing, without placing the information under seal, then the filing party must provide prior notice of its intention to do so sufficiently in advance under the circumstances to permit the producing party a reasonable opportunity to review the Protected Information and determine whether to approve the removal of the confidentiality designations or otherwise approve the filing of the materials without placing them under seal. If the filing party does not provide such notice, or if the producing party objects to the filing of its Protected Material without placing

them under seal, then the filing party must file a sealing motion simultaneously with such pleading or document, requesting that such Protected Information be filed under seal in accordance with the procedures set forth in any applicable local civil rules. The producing party must provide reasonable assistance to the filing party to support the sealing motion.

F. Disclosure of Protected Information to Technical Advisers

1. Information designated by the producing party as Protected Information and such copies of this information as are reasonably necessary for maintaining, defending, or evaluating this litigation may be furnished and disclosed to the receiving party's technical advisers and their necessary support personnel.

2. No disclosure of Protected Information to a technical adviser or his/her necessary support personnel shall occur until that technical adviser has signed the form attached hereto as Attachment A, and a signed copy has been provided to the producing party; and to the extent there has been an objection asserted in compliance with paragraphs I.F.4-I.F.5, that objection is waived or resolved either by agreement of the party engaging the technical adviser and the party objecting to disclosure of Protected Information to such person, or according to the provisions set forth below.

3. A party desiring to disclose Protected Information to a technical adviser shall give prior written notice of the intended disclosure by email to all counsel of record in the litigation, including the following information for each technical adviser: 1) the general categories of Protected Information (e.g., technical materials, financial statements, licensing materials, etc.) that the Receiving Party seeks permission to disclose to the technical adviser; 2) the technical adviser's full name and address; 3) a current curriculum vitae; 4) current employer(s); 5) each person or entity from whom the technical adviser has received direct compensation for work in his or her areas of expertise or to whom the expert has provided professional services, including in connection with a litigation, at any time during the preceding three years; and 6) a listing of cases (by name and number of the case, filing date, and location of court, if known to the technical adviser) in which the technical adviser has offered expert testimony, including through a

declaration, report, or testimony at a deposition or trial, within the preceding four years. To the extent the technical adviser is unable to disclose the specific employment because of any confidentiality obligations, the advisor shall disclose the time frame, general industry, and any other information sufficient to describe the engagement as permitted by the confidentiality obligations.

4. The producing party shall have five (5) business days after such notice is given to email any objection to the disclosure to all outside counsel of record for the party desiring to disclose Protected Information to a technical adviser. Any objection to disclosure to a technical adviser that is not emailed to outside counsel within this time period is waived, and the Protected Information may be disclosed to the technical adviser pursuant to the terms of this Order. No Protected Information shall be disclosed to such expert(s) or consultant(s) until after the expiration of the foregoing five business day notice period.

5. A party objecting for good cause to disclosure of Protected Information to a technical adviser shall state with particularity the ground(s) of the objection and the specific categories of documents that are the subject of the objection. The objecting party's consent to the disclosure of Protected Information to a technical adviser shall not be unreasonably withheld, and for the purposes of this subsection, "good cause" is an objectively reasonable concern as defined in Paragraph I.F.7 below.

6. Immediately upon emailing any objection to disclosure of Protected Information to a technical adviser, the producing party will make its counsel available to meet and confer, which meet and confer shall be concluded promptly and in no event later than two (2) business days following the transmission of the objection, unless another time is agreed to by the receiving and producing parties in writing. If after meeting and conferring the involved parties cannot resolve the objection (where such meet-and-confer need not take place in person), the objecting party may, within five (5) business days of the meet and confer, (a) seek an emergency ruling on the objection from the Court; or (b) file a motion seeking Court resolution of the objection. A failure to file a motion within the five (5) business day period, absent an agreement

of the parties to the contrary or for an extension of such period, shall operate as an approval of disclosure of Protected Information to the technical adviser. The parties agree to cooperate in good faith to shorten the time frames set forth in this paragraph if necessary to abide by any discovery or briefing schedules. Nothing stated herein shall hinder the ability of the party desiring to disclose Protected Information to a technical adviser to seek an emergency ruling or other relief with respect to the objection, and either party will be entitled to seek such emergency relief.

7. The objecting party shall have the burden of showing to the Court "good cause" for preventing the disclosure of its Protected Information to the technical adviser. This "good cause" shall include a particularized showing that: (1) the Protected Information is confidential technical or commercial information, (2) disclosure of the Protected Information likely would result in a clearly defined and serious injury to the objecting party's business, and (3) that disclosure of Protected Information to the proposed technical adviser would likely result in the Protected Information being disclosed to the objecting party's competitors, or other particularized, substantiated injury to the objecting party.

G. Challenges to Confidentiality Designations.

1. The parties shall use reasonable care when designating documents or information as Protected Information. Nothing in this Order shall prevent a receiving party from contending that any documents or information designated as Protected Information have been improperly designated. A receiving party may at any time request that the producing party withdraw or modify the Protected Information designation with respect to any document or information contained therein.

2. A party shall not be obligated to challenge the propriety of a designation of any category of Protected Information at the time of production, and a failure to do so shall not preclude a subsequent challenge thereto. Such a challenge shall be written, shall be served on counsel for the producing party, and shall particularly identify the documents or information that the receiving party contends should be differently designated. The parties shall use their best efforts to promptly and informally resolve such disputes. If an agreement cannot be reached, the

receiving party may request that the Court strike or modify a designation. The burden of demonstrating the confidential nature and appropriate designation of any information shall at all times be and remain on the producing party.

3. Until a determination by the Court, the information in issue shall be treated as having been properly designated and subject to the terms of this Order.

H. Limitations on the Use of Protected Information

1. All Protected Information shall be held in confidence by each person to whom it is disclosed, and shall not be disclosed to any person who is not entitled to receive such information as herein provided. All Protected Information shall be carefully maintained so as to preclude access by persons who are not entitled to receive such information. Protected Information designated under the terms of this Protective Order shall be used by a receiving party solely for this litigation and related lawsuits, and shall be used only for purposes of litigating this case, and related lawsuits, and shall not be used directly or indirectly for any other purpose whatsoever.

2. Depositions and Trial. Except as may be otherwise ordered by the Court, any person may be examined as a witness at deposition and trial and may testify concerning all Protected Information of which such person has prior knowledge. Without in any way limiting the generality of the foregoing:

a. A present officer, director, agent, contractor and/or employee of a producing party may be examined concerning all Protected Information which has been produced by that party.

b. A former officer, director, agent, contractor and/or employee of a producing party may be interviewed, examined and may testify concerning all Protected Information that constitutes or refers to matters of which the witness is believed in good faith to have relevant knowledge, which has been produced by that party and which pertains to the period or periods of his or her employment; and

c. Non-parties may be examined or testify concerning any document

containing Protected Information of a producing party which appears on its face or from other documents or testimony to have been received from or communicated to the non-party as a result of any contact or relationship with the producing party or a representative of the producing party. Any person other than the witness, his or her attorney(s), or any person qualified to receive Protected Information under this Order shall be excluded from the portion of the examination concerning such information, unless the producing party consents to persons other than qualified recipients being present at the examination. If the witness is represented by an attorney who is not qualified under this Order to receive such information, then prior to the examination, the attorney must provide a signed statement, in the form of Attachment A hereto, that he or she will comply with the terms of this Order and maintain the confidentiality of Protected Information disclosed during the course of the examination. In the event that such attorney declines to sign such a statement prior to the examination, the producing party, by its attorneys, may seek a protective order from the Court prohibiting the attorney from disclosing Protected Information, and the other parties shall not oppose such request.

3. Protected Information shall not be copied or otherwise produced by a receiving party, except for transmission to qualified recipients, except under the terms of this Order, without the written permission of the producing party, or, in the alternative, by further order of the Court. Except as otherwise provided, however, nothing herein shall restrict a qualified recipient from making working copies, abstracts, scans, digests and analyses of CONFIDENTIAL and CONFIDENTIAL OUTSIDE COUNSEL ONLY information for use in connection with this litigation and such working copies, abstracts, scans, digests and analyses shall be deemed Protected Information under the terms of this Order. Further, nothing herein shall restrict a qualified recipient from converting or translating CONFIDENTIAL and CONFIDENTIAL OUTSIDE COUNSEL ONLY information into machine readable form for incorporation into a data retrieval system used in connection with this action, provided that access to that Protected Information, in whatever form stored or reproduced, shall be limited to qualified recipients.

I. Inadvertent Production of Protected Information Without

Confidentiality Designation.

1. Inadvertent or unintentional production of documents or things containing Protected Information which are not designated as Protected Information at the time of production shall not be deemed a waiver in whole or in part of a claim for confidential treatment. With respect to documents, the producing party shall immediately upon discovery notify the other parties of the error in writing and provide replacement pages bearing the appropriate confidentiality legend. In the event of any disclosure of Protected Information other than in a manner authorized by this Protective Order, including any unintentional or inadvertent disclosure, counsel for the party responsible for the disclosure shall immediately notify opposing counsel of all of the pertinent facts, and make every effort to further prevent unauthorized disclosure, to retrieve all copies of the Protected Information from unauthorized recipient(s) thereof, and to secure the agreement of the unauthorized recipients not to further disseminate the Protected Information in any form. Compliance with the foregoing shall not prevent the producing party from seeking further relief from the Court.

J. Protected Information Requested to Be Produced Outside This Litigation.

1. If at any time documents containing Protected Information are subpoenaed by any court, arbitral, administrative or legislative body, or are otherwise requested in discovery, the person to whom the subpoena or other discovery request is directed shall promptly give written notice thereof to counsel for every party who has produced such documents with the objective of providing each such party with an opportunity to object to the production of such documents and seek appropriate relief. If a producing party does not take steps to prevent disclosure of such documents within 10 business days of the date written notice is given or in time to get an order excusing production of the Protected Information before the production is called for by the subpoena or other request, the party to whom the referenced subpoena or request is directed may produce such documents in response thereto.

2. In the event that the producing party intends to seek such an order to prevent disclosure, the producing party shall promptly so advise the party receiving the subpoena or other

discovery request, who shall bear no liability or responsibility to the extent that such notice is not delivered on a timely basis. Nothing herein shall be construed as requiring the party receiving the subpoena or other request to file a motion excusing its production of the Protected Information, to challenge or appeal any order requiring production of information or material covered by this Protective Order, to violate a subpoena or other lawful request for production, or to subject itself to any penalties for noncompliance with any legal process or order, or to seek any relief from the discovery request.

K. Destruction of Protected Information After Suit Ends.

1. After final resolution of the case as to any party producing Source Code, any receiving parties shall within thirty (30) business days certify the return or destruction of any printed or duplicated Source Code material.

2. Within 90 days after the entry of a final non-appealable judgment or order, or the complete settlement of all claims asserted against all parties in this action, each party shall, at the option of the receiving party, either return or destroy all physical objects and documents which embody any remaining Protected Information it has received.

3. In the event that a party is dismissed before the entry of a final non-appealable judgment or order, this same procedure shall apply to any Protected Information received from or produced to the dismissed party, including the destruction or return due date of 90 days after the entry of a final non-appealable judgment or order resolving the entire case as against all parties, or the complete settlement of all claims asserted against all parties in this action.

4. Notwithstanding the provisions of Section I.K.2, above, outside litigation counsel of record are not required to delete information that may reside on their respective firm's electronic back-up systems that are over-written in the normal course of business, and outside counsel shall be entitled to maintain copies of all pleadings, motions and trial briefs (including all supporting and opposing papers and exhibits thereto), written discovery requests and responses (and exhibits thereto), deposition transcripts (and exhibits thereto), trial transcripts, expert reports, and exhibits offered or introduced into evidence at any hearing or trial, and their attorney work

product which refers or is related to any CONFIDENTIAL and CONFIDENTIAL OUTSIDE COUNSEL ONLY information for archival purposes only.

L. Nonparties to the Litigation

1. A nonparty producing information or material voluntarily or pursuant to a subpoena or a court order may designate such material or information as Protected Information pursuant to the terms of this Order, and may invoke its protections and restrictions over the nonparty's Protected Information. To the extent that such nonparty seeks the protections of this Order, it will also be subject to its obligations and deadlines.

2. A nonparty's use of this Protective Order to protect its Protected Information does not entitle that nonparty access to the Protected Information produced by any party in this case.

II. PROSECUTION BAR

1. "Prosecution Bar Materials" mean all CONFIDENTIAL INFORMATION, CONFIDENTIAL OUTSIDE COUNSEL ONLY materials or RESTRICTED CONFIDENTIAL – SOURCE CODE materials produced by a party or a non-party EXCEPT for (i) documents and information not of a technical nature; and (ii) information that is or becomes publicly available, including patents and published patent applications.

2. Any person who has reviewed opposing producing party's Prosecution Bar Materials shall not, for a period commencing upon receipt of such information and ending two (2) years following the conclusion of this case (including any appeals) engage in any Prosecution/Acquisition Activity (as defined below) on behalf of a party in this case or non-party.

3. Prosecution/Acquisition Activity shall include any activity related to the prosecution or acquisition of patents or patent applications relating to: 1) e-commerce technology for searching, displaying, advertising, offering, and/or selling products and/or services, or 2) traffic control technology for interfacing members for video communication over dial-up telephone. For purposes of this paragraph, "prosecution" includes directly or indirectly drafting, amending, advising on, or otherwise affecting the scope or maintenance of patent claims. Prosecution

includes, for example, original prosecution, reissue, reexamination, or other proceedings affecting the scope or maintenance of patent claims, including *inter partes* review or covered business method review. To avoid any doubt, "prosecution" as used in this paragraph does not include representing a party challenging a patent before a domestic or foreign agency (including, but not limited to, a reissue protest, *ex parte* reexamination or *inter partes* reexamination, *inter partes* review, or covered business method review). Nothing in this paragraph shall prevent any attorney from sending non-confidential prior art, without additional input or consultation, to an attorney involved in patent prosecution for purposes of ensuring that such prior art is submitted to the U.S. Patent and Trademark Office (or any similar agency of a foreign government) to assist a patent applicant in complying with its duty of candor. For purposes of this paragraph, "acquisition" means the acquisition of patents (including patent applications) or any exclusive rights to patents or patent applications with subject matter relating to: 1) e-commerce technology for searching, displaying, advertising, offering, and/or selling products and/or services, or 2) traffic control technology for interfacing members for video communication over dial-up telephone. Nothing in these provisions is intended to preclude counsel from participating in activities directly for the purpose of settling litigations.

4. Notwithstanding the provisions in Section II.1-II.3, the receiving party may seek leave from this Court for litigation counsel, experts and/or consultants to participate in reexamination proceedings (including *inter partes* review and covered business method review) brought by the producing party. Additionally, Telebuyer may seek leave of Court to exempt particular individuals from the prosecution/acquisition bar, such exemptions to be considered on an individual basis.

III. PRIVILEGED INFORMATION.

A. Limits on Waiver of Privilege.

1. Nothing in this Order shall require production of information that a party contends is protected from disclosure by the attorney-client privilege, the work product immunity or other privilege, doctrine, right, or immunity. The production of a document that is privileged or

otherwise protected from discovery does not result in the waiver of that privilege or protection in this litigation or any other federal or state proceeding, so long as such production is inadvertent and the producing party claws back the inadvertently produced document within a reasonable time after discovery of the inadvertent disclosure. Any party that inadvertently produces materials protected by the attorney-client privilege, work product privilege, or other privilege, doctrine, right, or immunity may obtain the return of those materials by promptly notifying the recipient(s) and providing a privilege log for the produced materials. The recipient(s) shall promptly gather and return, or destroy, all copies of the privileged material to the producing party.

2. Such return or confirmation of destruction shall not preclude the receiving party from seeking to compel production of such documents, and shall not constitute an admission by the receiving party that any such document was, in fact, privileged or protected in any way. The producing party shall retain the documents for submission to the Court in the event the receiving party moves to compel their production.

3. The parties agree that all attorney-client communications and work product created after the filing date of the earliest-filed complaint in this action are presumptively protected from disclosure at least by the attorney-client privilege and/or the attorney work product doctrine, and shall not be identified on privilege logs in connection with this action.

IV. LIMITS ON DISCOVERABILITY OF EXPERT MATERIALS.

1. Testifying and consulting experts shall not be subject to discovery of any draft of their reports in this case and such draft reports, notes, outlines, or any other writings leading up to an issued report(s) in this litigation are exempt from discovery. In addition, all communications to and from a testifying or consulting expert, and all materials generated by a testifying or consulting expert with respect to that person's work, are exempt from discovery unless actually relied upon by the testifying expert in forming any opinions in this litigation and such information is not already disclosed in the expert's report. The foregoing does not otherwise restrict discovery by oral deposition of testifying experts, does not obligate any party to retain draft reports, and is not intended in any way to narrow the protections regarding disclosure of expert

materials in Fed. R. Civ. P. 26.

V. MISCELLANEOUS

1. This Order is entered without prejudice to the right of any party to apply to the Court at any time for additional protection, or to relax or rescind the restrictions of this Order, or otherwise modify this Order, when convenience or necessity requires. This Order is not intended to prevent a party from seeking additional protections outside of this Order prior to production of Protected Information, when convenience or necessity requires. Furthermore, without application to this Court, any party that is a beneficiary of the protections of this Order may agree to release any other party hereto from one or more requirements of this Order even if the conduct subject to the release would otherwise violate the terms herein.

2. This Court is responsible for the interpretation and enforcement of this Order. Following termination of this litigation, the provisions of this Order shall continue to be binding except with respect to those documents and information that become a matter of public record. This Court retains and shall have continuing jurisdiction over the parties and recipients of the Protected Information for enforcement of the provision of this Order following termination of this litigation. All disputes concerning Protected Information produced under the protection of this Order shall be resolved by this Court.

3. Nothing in this Order shall preclude or impede outside litigation counsel of record's ability to communicate with or advise their respective clients in connection with this litigation only based on such counsel's review and evaluation of Protected Information, provided however, that such communications or advice shall not disclose or reveal the substance or content of any Protected Information other than as permitted under this Order.

4. Each of the parties agrees to be bound by the terms of this Order as of the date counsel for all parties have emailed each other that they approve the terms of this Order, even if prior to entry of this order by the Court.

5. Nothing in this Order shall prevent any party from disclosing materials in which all Protected Information has been redacted to an individual or nonparty not designated

under this Order to receive Protected Information, but only to the extent the producing party verifies that such Protected Information has been properly redacted, which verification shall be performed within a reasonable time.

6. Headings in this Order are for ease of reference only and not intended to alter the provisions of the Order.

7. Any person may be examined as a witness at trial, a hearing or during a deposition concerning any CONFIDENTIAL INFORMATION which that person had lawfully received or authored prior to and apart from this action and, therefore, nothing in this Order shall preclude any Party to this lawsuit or their attorneys from: (1) showing a document designated as "CONFIDENTIAL INFORMATION," "CONFIDENTIAL OUTSIDE COUNSEL ONLY," or "RESTRICTED CONFIDENTIAL – SOURCE CODE" to an individual who either authored or was copied on the distribution of the document, as indicated on the document's face; or (2) from disclosing or using, in any manner or for any purpose, any information or documents from the Party's own files which the Party itself has designated as "CONFIDENTIAL INFORMATION," "CONFIDENTIAL OUTSIDE COUNSEL ONLY," or "RESTRICTED CONFIDENTIAL – SOURCE CODE" provided, however, that such a disclosure or use may be argued by the receiving party to constitute a waiver of the producing party's right to maintain such designations.

8. By stipulating to the entry of this Order, no party waives any right it otherwise would have to object to disclosing or producing any information or item. Similarly, no party waives any right to object on any ground to the use in evidence of any of the material covered by this Order. The parties' agreement to this Order shall not constitute a waiver of the right of any party to claim in this action or otherwise that any material, or any portion thereof, is privileged or otherwise nondiscoverable, or is not admissible in evidence in this action or any other proceeding.

ENTERED this 7th day of August, 2014.

Barbara J. Rothstein

UNITED STATES DISTRICT JUDGE

ATTACHMENT A
CONFIDENTIALITY AGREEMENT

My name is _____.

1. I reside at _____.

2. My present employer is _____.

3. My present occupation or job description is _____.

4. I have read the Protective Order dated _____, 20___, and have been engaged as _____ on behalf of _____ _____ in the preparation and conduct of the above-captioned litigation.

5. I am fully familiar with and agree to comply with and be bound by the provisions of said Order. I submit to, and waive any objection I may have to, the jurisdiction of the United States District Court for the Western District of Washington to enforce the terms of the Protective Order, including after such time as the case may be concluded. I understand that I am to retain all copies of any documents designated as CONFIDENTIAL, CONFIDENTIAL OUTSIDE COUNSEL ONLY and/or RESTRICTED CONFIDENTIAL – SOURCE CODE, or any similar designation, in a secure manner, and that all copies are to remain in my personal custody until I have completed my assigned duties, whereupon the copies and any writings prepared by me containing any information designated CONFIDENTIAL, CONFIDENTIAL OUTSIDE COUNSEL ONLY and/or RESTRICTED CONFIDENTIAL – SOURCE CODE, or any similar designation, are to be returned to counsel who provided me with such material.

6. I will not divulge to persons other than those specifically authorized by said Order, and will not copy or use except solely for the purpose of this action, any information obtained pursuant to said Order, except as provided in said Order. I also agree to notify any stenographic or clerical personnel who are required to assist me of the terms of said Order.

7. I state under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on _____, 20____.

_____