Exhibit C

Google Inc.'s Briefing in Support of Entry of a Protective Order

Exhibit C: Defendant's Statement

Defendant respectfully submits its arguments in support of its positions on the disputed issues in the parties' proposed Protective Order. Plaintiff's suggestion that its proposals follow the Court's model Protective Order, and Defendant's do not is misleading. Both parties propose deviating from the model order in certain instances. For example, Plaintiff's proposal regarding mock juror accessibility to Defendant's Designated Material is not supported by the model order. And, Plaintiff admits that it deviates from the model order with respect to the prosecution bar. Plaintiff similarly took provisions from the various protective orders from other cases to which it cites to find support for its various positions. As cited below, many of those very same cases support Defendant's positions as well. In all events, there is good cause for the protections Defendant seeks for its confidential and sensitive information, and where Defendant's proposals vary from the terms of the model order, they are warranted under the circumstances of the case and do not unjustifiably hamper discovery.

I. DISPUTES REGARDING SOURCE CODE REVIEW

Defendant proposed certain safeguards to balance protection of its confidential and proprietary source code with Plaintiff's ability to conduct its review of that source code in an efficient manner. *See e.g.*, *E-Contact Technologies, LLC v. Apple, Inc.*, Case No. 1:11-cv-00426-LED-KFG (E.D. Tex. June 19, 2012), D.I. 344, at 7 (recognizing the importance of protecting source code). Although the parties resolved many issues concerning source code review, the following three provisions concerning review of Defendant's highly confidential and proprietary source code remain in dispute.

A. A Personal Laptop Should Not Be Permitted in the Secure Source Code Review Environment (Paragraph 11(a))

The parties have agreed that source code will be loaded onto two non-networked computers that are password protected and maintained in a secure, locked area for inspection. (*See* Proposed Protective Order, ¶ 11(a).) The parties have also agreed that use or possession of any input/output devices, including USB memory sticks, cameras or any camera-enabled device, CDs, floppy disk, portable hard drive, or any devices that can access the Internet or any other network or external system are prohibited while accessing the computers containing the source code. (*Id.*) The issue in dispute is whether use or possession of a personal laptop computer additionally may be permitted in the secure, locked area where source code inspection occurs, as requested by Plaintiff. (*Id.*)

Permitting a personal laptop in the locked area, however, would undermine the parties' agreement to exclude input/output devices. Having a personal laptop in the source code review room in view of the source code inspection computers, even if it is not connected to a network, will make it easier for an expert or consultant to copy the code into a document on the laptop, in violation of the Protective Order. (*See* ¶ 11(c)) ("The Receiving Party's outside counsel and/or expert or consultant shall be entitled to take notes relating to the Source Code but may not copy any portion of the Source Code into the notes.")(emphasis added). This is why courts in this District routinely bar any and all personal computer use in the secure source code inspection area. *See, e.g., Geotag Inc. v. Frontier Commc'ns Corp.,* Case No. 10-0570 (E.D. Tex. Jan. 8, 2013) (denying plaintiff's request that a note-taking computer be allowed within the secure source code room; "The Court is unconvinced that sufficient review of Defendants' source code requires a cellular telephone or note-taking computer. In light of the highly confidential nature of the source code, allowing these devices within the secure room would significantly increase the possibility of inadvertent disclosure."); *Blue Calypso, Inc. v. Groupon*, Case No. 6:12-cv-486, D.I. 160 (E.D. Tex. Oct. 29, 2013), ¶ 8f (precluding the use of computers in the source code review room, and explicitly providing that notes cannot be taken "electronically on the Source Code Computer or any other computer"); *E-Contact Technologies, LLC v. Apple, Inc.*, Case No. 1:11-cv-00426-LED-KFG, D.I. 344 (E.D. Tex. June 19, 2012), at 7-8 (denying the plaintiff's request to be allowed to take notes on a laptop during source code review); *Eolas Techs. Inc. v. Adobe Sys Inc.*, Case No. 6:09-cv-00446-LED, D.I. 423 (E.D. Tex. Sept. 10, 2010), ¶ 13(b)(iii) (precluding the use of personal computers in the source code review room) . Moreover, Plaintiff's proposal would not even prevent someone reviewing source code from taking pictures of the source code with the laptop's camera.

Plaintiff's stated basis for seeking to bring a personal computer into the secure review environment is simply that it will facilitate its consultants' and experts' review of Defendant's source code because it will allow for them to take notes while reviewing the source code, search their own materials for information, revise claim charts, and draft sections of reports. But, as cited above, courts in this District routinely preclude the use of personal computers in source code review rooms, and have explicitly rejected this as a grounds for allowing a personal laptop in a source code inspection room. *See Geotag Inc.*, Case No. 10-0570 (E.D. Tex. Jan. 8, 2013); *E-Contact*, Case No. 1:11-cv-00426-LED-KFG, D.I. 344, at 7-8.

Plaintiff attempts to distinguish *E-Contact*, arguing that there the plaintiff could print the source code and take it to a laptop to prepare work product. But, in this case, nothing precludes the receiving party or its experts or consultants from taking written notes in compliance with the Protective Order to a laptop nearby, such as a guest office, to create the expert or consultant's work product. That it takes more time to take "handwritten notes with pen and paper" does not warrant significantly increasing the possibility of inadvertent disclosure and copying of source code by allowing a personal laptop in the secure source code inspection room.

Plaintiff also cites to *Bluebonnett Telecomms. LLC v. Sony Ericsson Mobile Communications (USA) Inc.*, No. 2 :13-cv-00505-JRG (E.D. Tex), but that case is distinguishable. There, the plaintiff argued that it needed access to a personal laptop during source code inspections because some of the source code was public, so the experts and consultants needed to be able to compare the source code on the inspection computers to the public code. *Id.* D.I. 25. That is not the case here.

Further, Defendant already addressed Plaintiff's concerns regarding facilitating source code review. It agreed to allow Plaintiff access to two standalone source code inspection computers, rather than one, because Plaintiff represented that this additional access would facilitate the source code review. Thus, an additional personal computer is not necessary. Additionally, Plaintiff's paid consultants and experts presumably are experienced professionals capable of efficiently conducting review and analysis of source code on two non-networked computers without increasing the risk of inadvertent disclosure through the use of a third, personal computer in the secure source code inspection area.

Lastly, Plaintiff argues that Defendant has been subject to Protective Orders that permit the use of a personal laptop in the source code inspection room without any resulting harm. Defendant, however, should not have to wait for harm to occur to maintain the security of its highly sensitive source code. As Plaintiff points out, it has accused a broad swath of Defendant's products and services, including its very successful search and advertising services. If the source code for these products and services were to be used improperly, it could be catastrophic to

Defendant's business. Thus, it is entirely reasonable to preclude the use of a laptop during source code inspection as supported by Defendants' cited authority.

B. **The Number of Pages of Printouts of Source Code Should be Limited (Paragraph 11(g))**

Defendant proposes that the Protective Order also include the provision that "in no event may Rockstar print more than 25 consecutive pages, or an aggregate total of more than 500 pages, of source code during the duration of the case without prior written approval by the producing party." (*See* Proposed Protective Order, ¶ 11(g).) And, Defendant's proposal further makes clear that Defendant will not unreasonably withhold written approval to exceed the permitted number of printed pages of source code. *Id.* Plaintiff does not agree to such a restriction. *Id.*

Plaintiff's desire to be entitled to an essentially unlimited number of printed pages of source code is unacceptable. The protection of Defendant's source code is of paramount importance, and Plaintiff's outside counsel and approved experts and consultants will have ample opportunity to review Defendant's source code on the secure computers. Thus, printing of source code should be kept to an absolute minimum. This is true of both the aggregate number of pages printed, and the number of consecutive pages printed. Restrictions on the latter are just as important as limitations on the aggregate number of pages because they prevent the existence of a printout of an entire program that could then be easily implemented by a competitor. The imposition of page limits on printing of source code, as proposed by Defendant, is both necessary and non-controversial. *See, e.g., E-Contact Tech., LLC v. Apple, Inc.*, Case No. 11-0426, D.I. 344 (E.D. Tex. June 19, 2012), at 7 (adopting Defendants' proposal that "Plaintiff should only be able to print 10 consecutive pages and 500 aggregate pages of source code"); *see also MicroUnity v. Acer*, No. 2:10-cv-00091-TJW, D.I. 304 (E.D. Tex., Aug. 23, 2011), ¶ 11(a) (limiting the receiving party from printing no more than 10 consecutive pages of source code, stating that no more than 10% or 500 pages of the total amount of source code available, whichever is less, may be in printed form at any one time, and providing that the receiving party may request additional printed pages and the producing party shall not unreasonably deny such request).

Plaintiff contends that it should not be limited to an "arbitrary" limit of source code printouts, but rather should only be limited to a "reasonable number of pages" because it broadly accuses "at least a dozen accused instrumentalities"[1] and does not yet know how many pages it will need. In the first instance, Defendant's proposal is not "arbitrary." It is consistent with the limitations in *E-Contact* and *Superspeed, LLC v. Google*, cited by Plaintiff. *Superspeed, LLC v. Google Inc.*, Case No. 4:12-cv-01688, D.I. 38 (S.D. Tex. Jan. 10, 2013), ¶ 3.B.(iv). Moreover, that Plaintiff's infringement case asserting well over one-hundred claims against Defendant is overbroad does not justify an unlimited number of printouts of Defendant's source code. In any event, to alleviate Plaintiff's concerns regarding not yet knowing how many pages of source code it will need, and in an effort to reach a compromise, Defendant suggested that Plaintiff can return printed pages of source code that it no longer needs and Defendant will credit that page count back to Plaintiff. Neither of the cases by Plaintiff include such a provision. Plaintiff, however, rejected this offer.

Plaintiff's position also disregards that Defendant's proposal specifically allows for printing of additional pages upon prior written approval and that Defendant's approval "will not unreasonably be withheld." And, even if written approval were not provided, nothing precludes Plaintiff from seeking relief from the Court if it determines, after reaching the limit of 25

[1] That Plaintiff does not know how many products it accuses of infringement illustrates the improper nature of its specific infringement contentions to date.

consecutive pages or 500 aggregate pages of source code printouts, that it legitimately needs more. Plaintiff contends that this will only ensure more motion practice. Not so. Even if Plaintiff's proposal is accepted, there is no guarantee that the parties will agree on what is a "reasonable" number of printed pages of source code. Defendant's proposal provides guidelines which should minimize additional motion practice.

Finally, Plaintiff again argues that Defendant has been subject to Protective Orders that did not include numerical printing limits for source code without any resulting harm. Once again, Defendant should not have to wait for harm to occur in order to maintain the security of its highly sensitive source code. The Court should limit the printing of source code as proposed by Defendant.

C. **Source Code Should Only be Transported by Hand. (Paragraph 11(j))**

The parties agree that materials designated "RESTRICTED CONFIDENTIAL SOURCE CODE" shall be stored or viewed at a limited set of locations, and agree on those locations and that they shall be maintained at all times in a secure location under the direct control of an approved expert or consultant, or counsel. (*See* Proposed Protective Order, ¶ 11(j).) Plaintiff, however, proposes a disclaimer that nothing precludes the receiving party "from mailing, shipping, or delivering source code" between the approved locations. But this language completely undermines the provision that Rockstar agreed to—that source code remain in the direct control of approved experts or consultants, or counsel.

For example, Plaintiff's proposal would allow it to put printed copies of Defendant's highly sensitive source code into the U.S. Mail. U.S. Mail is not under the direct control of anyone associated with this case or under the Protective Order. Indeed, if the printed source code is lost in the mail, there will be no one who can answer for where it went, who obtained access to it, etc. The same is true of other services, like FedEx, that Plaintiff may use to mail, ship, or deliver source code. Even if they offer tracking services, there is not a single person responsible for the constant security of the code.

Plaintiff argues that this provision should be included because Plaintiff should not be required to hand-deliver printed copies of source code to its approved experts or consultants. Defendant does not insist that counsel hand-deliver source code printouts. Rather, counsel can retain a courier to make these deliveries. That courier can ensure that the printed source code is delivered to the right person and that Defendant's most sensitive materials are adequately protected for the entirety of the trip. And, that person can answer any questions that may arise if something unexpected occurs in transit. This does not impose an onerous burden on Plaintiff, and any burden is greatly outweighed by the importance of maintaining the security of Google's source code. Moreover, nothing precludes Plaintiff's approved experts and consultants from reviewing printed pages of source code in counsel's offices, altogether eliminating the need to transport them.

II. DISPUTES REGARDING ACCESS TO DESIGNATED MATERIAL

A. In-House Counsel Should Not Have Access to "RESTRICTED – ATTORNEYS' EYES ONLY" or "RESTRICTED – ATTORNEYS' EYES ONLY – PROSECUTION BAR" Information (Paragraph 10)

Plaintiff is a non-practicing entity in the business of acquiring patents and filing lawsuits to collect licensing revenues. Some of Defendant's major competitors, including Apple and Microsoft, are members of Plaintiff. Thus, it is important in this case that Defendant's highly confidential information not be accessible to anyone internally at Plaintiff. Especially given Plaintiff's ownership, there is significant potential for competitive danger to Defendant if its "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material is accessible internally at Plaintiff. Thus, the circumstances of this case warrant a departure from the Court's model Protective Order on this issue. Departure from the model order on this issue is not unprecedented, as evidenced by several of the cases cited by Plaintiff. *See MicroUnity v. Acer*, No. 2:10-cv-00091-TJW, Dkt 244-2, 244-3, D.I. 304 (E.D. Tex., Aug. 23, 2011), ¶ 10 (not granting in-house counsel access to highly confidential information); *PersonalWeb Technologies, LLC v. NEC Corp. of America*, No. 6:11-CV-00656, D.I. 89 (E.D. Tex., Aug. 7, 2012), ¶ I.B.2. (in-house counsel does not have access to Outside Counsel's Eyes Only material); *Blue Calypso, Inc. v. Groupon*, No. 6:12-cv-486, D.I. 160 (E.D. Tex., Oct. 24, 2013), ¶ 5 (not granting in-house counsel access to highly confidential information); *Eolas Techs. Inc. v, Adobe Sys. Inc.*, Case No. 6:09-cv-00446-LED, D.I. 423 (E.D. Tex., Sept. 10, 2010), ¶ 9(c) (same).

Plaintiff does not refute that the nature of its business or its ownership present a danger to allowing in-house counsel to see "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material. Rather, Plaintiff contends that disclosure to in-house counsel is acceptable because its counsel will not exercise competitive decision-making authority on behalf of the client. (*See* Proposed Protective Order, ¶ 10.)

Before granting counsel access to an opposing party's highly confidential information, however, courts in this District consider who the counsel are and their duties. For example, in *Life Technologies Corp. v. Biosearch Technologies, Inc.*, 2001 WL 1157860 (E.D. Tex. Mar. 29, 2011), the Court granted in-house counsel access to the opposing party's highly confidential information _only_ after an analysis of the specific individual counsel's activities, association, and relationship with the party. *See also Nike, Inc. v. Adidas America, Inc.,* Case No. 9:06–cv–43 (E.D.Tex. Sept. 21, 2006), D.I. 58 (refusing to modify a protective order to grant in-house counsel access to confidential information because there was a substantial risk for inadvertent disclosure of trade secrets.). This is a particularly important inquiry for a patent holding and licensing company like Plaintiff, which very likely has attorneys who wear legal and business hats. *See e.g.*, *Diagnostic Systems Corp. v. Symantec Corp.*, 2008 WL 9396387, *5-6 (C.D. Cal. 2008) (describing how attorneys had both business and legal roles at company whose only business was "to analyze, investigate, and attempt to enforce the patents-in-suit").

Here, however, Plaintiff provided no facts that would justify allowing in-house counsel reviewing "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material. Plaintiff has not identified its in-house counsel. Plaintiff has provided no description of in-house counsel's actual responsibilities or roles, much less any explanation of how that in-house counsel could not and would not use Defendant's highly confidential information in other aspects of their jobs as in-house counsel for an entity owned by Google's competitors. Nor has Plaintiff provided any basis to allay Defendant's legitimate concern of inadvertent or unintentional disclosure or use of Defendant's "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material.[2] The risk of disclosure or use of such material is too high and outweighs any need for Plaintiff's in-house counsel to have access to the material.

[2] Causing Defendant more concern is that Plaintiff will not even have its in-house counsel commit to not engage in competitive decision making. During negotiations over the proposed Protective Order, Defendant asked Plaintiff if the designated in-house counsel would execute something confirming that they are not competitive decision-makers. Plaintiff's counsel responded:"[w]e are not willing to have in-house people sign any additional agreement or affirmation as it is unnecessary because they will be bound by the protective order." That Plaintiff is not willing to do so raises significant concerns regarding who Plaintiff wishes to show Defendant's "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material.

Moreover, Plaintiff cannot show that its ability to litigate this case will be hampered if in-house counsel do not have access to "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material. *See Brown Bag Software v. Symantec Corp.*, 960 2d. 1465, 1471 (9th Cir. 1992) (analyzing the risk of impairment of a party's case if its in-house counsel does not have access to the opposing party's confidential information). Plaintiff's outside counsel and its independent experts and consultants will have access to such information (under the terms of the Protective Order), so there is no reason why Plaintiff's in-house counsel must also have access. Indeed, just last week, Plaintiff agreed to a Protective Order in another matter against Defendant and others, under which its in-house counsel does <u>not</u> have access to such material. (*See Rockstar Consortium US LP et al. v. ASUSTeK Computer, Inc.*, Case No. 2:13-cv-00894-JRG, D.I. 108, (E.D. Tex. May 19, 2014), Ex. A-Proposed Protective Order, ¶ I.B.2.) When asked about this inconsistency, Plaintiff's counsel merely stated that the in-house counsel responsible for this case wants access to this material, with no further explanation. But, if Plaintiff can litigate the *ASUSTeK* case without its in-house counsel's access to "RESTRICTED – ATTORNEYS' EYES ONLY" and "RESTRICTED-ATTORNEYS' EYES ONLY-PROSECUTION BAR" material, there is no reason to believe it cannot do so here.

B. <u>Mock Jurors Should Not Have Access to Designated Material (Paragraphs 6(f) and 33)</u>

The parties dispute whether mock jurors shall have access to Designated Material. Defendant does not believe that they should. But, Plaintiff contends that it needs to disclose Defendant's Designated Material to mock jurors because without doing so, it cannot have a meaningful mock trial. In other words, Plaintiff's position is merely driven by its strategic desire to conduct a mock trial.

The Court should adopt Defendant’s proposal because mock jurors should not have access to Defendant’s Designated Material. It is entirely reasonable to minimize the dissemination of Defendant’s Designated Material. If used in a mock trial by Plaintiff, Defendant has no control over who will see its Designated Material; it does not control who the mock jurors are or what they are told. Indeed, Defendant will not even know that a mock trial was conducted until after it has already been conducted and if the case has not settled before the pretrial conference. Thus, Defendant has no opportunity to vet and police the conduct of the mock jurors—whose identities it will never know—selected by Plaintiff. (*See* Standing Order Regarding Mock Juries for Cases Assigned to Judge Rodney Gilstrap and Judge Roy S. Payne.)

Plaintiff has not identified any case law to Defendant that supports its request that mock jurors have access to Designated Material. The Court’s model Protective Order also does not grant mock jurors access to Designated Material. And, here too, Plaintiff agreed to a Protective Order in another matter, wherein mock jurors would not have access to Designated Material. (*See Rockstar Consortium US LP et al. v. ASUSTeK Computer, Inc.*, Case No. 2:13-cv-00894-JRG, D.I. 108 (E.D. Tex. May 19, 2014), Ex. A-Proposed Protective Order, ¶ I.A.6.e (giving access to “Confidential” information to “non-technical jury or trial consulting services not including mock jurors.”) There is no reason why mock jurors must have access to Designated Material here, but not in *ASUSTeK*. At best, Plaintiff cites to the Protective Order in *PersonalWeb*, where Defendant agreed that mock jurors could have access to “CONFIDENTIAL” information. But, the Protective Order there limited such access to only one tier—that of “CONFIDENTIAL” information. Plaintiff’s proposal does not; it would allow mock jurors to have access to RESTRICTED - ATTORNEYS' EYES ONLY," "RESTRICTED -

ATTORNEYS' EYES ONLY – PROSECUTION BAR," or "RESTRICTED CONFIDENTIAL SOURCE CODE" information.[3]

Plaintiff argues that its proposal protects Defendant's Designated Material by including specific provisions that must be followed before sharing Designated Material with mock jurors. (*See* Proposed Protective Order, ¶ 33.) But, these provisions do not eliminate Defendant's concerns for multiple reasons. Contrary to Plaintiff's claim that its proposal prohibits the viewing of Defendant's Designated Material, Plaintiff's proposal would allow Plaintiff to make "presentations" about Designated Material. When asked what this means, Plaintiff's counsel explained that if it identifies a "hot" document, it will put an image of that document in a PowerPoint presentation that will be shown to mock jurors. In other words, the mock jurors will see the actual Designated Material. Similarly, Plaintiff's proposal would allow it to play deposition testimony for jurors. But that testimony itself is Designated Material, not a mere summary of such material. Under Plaintiff's proposal, it could play the testimony of an engineer explaining the technical details of the "secret sauce" of how Defendant's search or advertising systems operate. This is highly sensitive information that should not be disseminated. Plaintiff's strategic plan to have a mock trial simply does not outweigh the importance of maintaining the confidentiality of Defendant's Designated Material.

C. <u>The Parties Should Jointly Prevent Third-party Attorney Access to Designated Material (Paragraph 12)</u>

The parties dispute whether the parties shall move jointly for a protective order in the event counsel for a non-party witness declines to join the protective order prior to the

[3] Plaintiff's proposal says "not including Source Code Material," and does not use the designation language used in the proposed Protective Order. Thus, it is difficult to know what Plaintiff does and does not intend to show to mock jurors with respect to source code. For example, a technical document or presentation could include a few lines of source code. Defendant cannot determine if this is the type of document Plaintiff would show mock jurors.

examination of that witness. The parties have an identical dispute in *Rockstar Consortium US LP et al. v. ASUSTeK Computer, Inc.*, Case No. 2:13-cv-00894-JRG, D.I. 108 (E.D. Tex. May 19, 2014). Defendant defers to the Court's ruling on this issue in that case.

III. DISPUTE REGARDING SCOPE OF PROSECUTION BAR

Plaintiff's counsel and its experts will have access to the highly confidential and proprietary information of Defendant. A prosecution bar prevents a patent holder from improperly (even if inadvertently) using a party's proprietary information during prosecution or post-grant challenge proceedings to modify claims so that they read on the disclosing party's products. As reflected in their proposals, the parties agree that a prosecution bar should apply to Plaintiff. The dispute that remains is whether it should apply to Prosecution Activity involving claims on a method, apparatus, or system directed to the technology of the patents-in-suit.

Defendant proposes that the prosecution bar should apply to (1) Prosecution Activity on behalf of a party asserting a patent in this case involving claims on a method, apparatus, or system directed to the technology of the patents-in-suit, and (2) Prosecution Activity involving claims on a method, apparatus, or system directed to the technology of the patents-in-suit, which is consistent with the prosecution bars in some of the cases cited by Plaintiff. *See PersonalWeb Technologies, LLC v. NEC Corp. of America*, case 6:11-CV-00656, D.I. 89, ¶ 2A; *Eolas Techs. Inc. v, Adobe Sys. Inc.*, Case No. 6:09-cv-00446-LED, D.I. 423, ¶ 5a. Plaintiff proposes that the prosecution bar should apply to Prosecution Activity on behalf of a party asserting a patent in this case or "its acquirer, successor, predecessor, or other affiliate." In other words, under Plaintiff's proposal, persons with access to prosecution bar materials would not be permitted to engage in Prosecution Activity on behalf of Rockstar, its acquirer, successor, predecessor, or affiliates (whatever that means) but would be permitted to do so on behalf of other entities.

Contrary to Plaintiff's arguments, the risk of use of Defendant's highly confidential information in patent prosecution is the same, regardless of who the represented party is. Thus, persons with access to Defendant's prosecution bar materials should not be able to engage in such Prosecution Activity for any entity. Again, this is particularly important in this case. Plaintiff is a consortium of several companies, including Defendant's competitors Apple and Microsoft. Unless these members are what Plaintiff considers its "affiliates," under Plaintiff's proposal, Rockstar's attorneys (as well as approved experts and consultants) with access to Defendant's prosecution bar materials would be free to engage in Prosecution Activity on behalf of Google competitors like Apple and Microsoft. Even if Prosecution Activity on behalf of these competitors were barred by Plaintiff's proposal, however, it would still allow for Prosecution Activity on behalf of any other entity, which risks the improper use of Defendant's prosecution bar materials.

Similarly, Defendant's proposed definition of "Prosecution Activity" includes "(3) provide advice, counsel or suggestions regarding, or in any other way influencing, claim scope and/or language, embodiment(s) for claim coverage, claim(s) for prosecution, or products or processes for coverage by claim(s) <u>on behalf of a patentee or assignee of patentee's rights</u>." (underlining added). Plaintiff's definition excludes this language because Plaintiff does not agree to the underlined portion. Again, Plaintiff contends that it should not be limited from providing advise influencing claim scope and/or language, etc., for parties other than Rockstar. But, as explained above, the danger of use of Defendant's highly confidential prosecution bar materials in advising on claims is the same, regardless of the represented party.

IV. DISPUTE REGARDING INCLUSION OF ACQUISITION BAR

Defendant proposes an acquisition bar because Plaintiff is a non-practicing entity in the business of acquiring patents and filing lawsuits to collect licensing revenues. It would be highly prejudicial to allow Plaintiff, who practices no patents and is in the business of filing lawsuits, to benefit from having access to Defendant's confidential information and to use that information to acquire patents to assert against Defendant's products and services. *See, e.g.*, *Unwired Planet LLC v. Apple Inc.*, No. 12-0505, 2013 WL 1501489, at *7 (D. Nev. Apr. 11, 2013) (finding that "good cause exists to include in the protective order the bar that Unwired's outside counsel cannot use the confidential information obtained in this lawsuit for the purpose of giving advice on patent acquisitions"); *E-Contact Technologies, LLC v. Apple, Inc.*, Case No. 1:11-cv-00426-LED-KFG (E.D. Tex. June 19, 2012), D.I. 344, at 3-4 ("This Court finds that the potential harm of inadvertent disclosure outweighs the restriction imposed on counsel for Plaintiff. An acquisition bar should be included in the protective order."); *see also PersonalWeb Technologies, LLC v. NEC Corp. of America*, case 6:11-CV-00656, D.I. 89, ¶ 2B (barring both prosecution and acquisition activity).

Defendant's proposed acquisition bar is narrowly tailored and a reasonable safeguard to ensure that any person reviewing any of its prosecution bar materials shall not, for a period of two years following the conclusion of this case, engage in any activity related to the acquisition of patents or patent applications or advising or counseling clients regarding the same. In other words, what it precludes is a person having access to Defendant's prosecution bar materials using that information, even if inadvertently, to acquire patents or applications, or advise clients regarding such acquisitions. This is not an attempt to escape infringement allegations or to stifle competition, as Plaintiff argues, but merely ensures that individuals with access to such information do not inadvertently use it improperly.[4]

[4] The parties' dispute in paragraph 9 citing to paragraphs 13 and 14 is tied to the dispute regarding the Acquisition Bar. Defendant's proposal includes a reference to the paragraphs

discussing the Prosecution Bar and the Acquisition Bar. Plaintiff's proposal references only the Prosecution Bar.