IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC., Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	)	Case No. 2:18-cv-00094-HCM-LRL

DEFENDANT CISCO SYSTEMS, INC.'S OBJECTIONS TO ISSUES RAISED AT APRIL 8, 2020 TELEPHONIC CONFERENCE AND MEMORANDUM IN SUPPORT OF ITS EXPEDITED MOTION OPPOSING TRIAL ENTIRELY BY VIDEOCONFERENCE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE

Cases

Rules

Defendant Cisco Systems, Inc. ("Cisco") respectfully submits this objection and expedited motion in response to two issues discussed at the April 8, 2020 teleconference in the above-captioned matter. These two issues are: (1) Cisco's written objection to the Court's plan to conduct the May 6, 2020 bench trial entirely by videoconference; and (2) Cisco's objection to the Court's consideration of the transcript from the partial Centripetal/Keysight trial, which is not part of the record of this case.

While videoconference is effective for some judicial proceedings and trials, this case is an exceptionally poor candidate for a trial by videoconference due its inherent complexities. This case involves five patents and allegations that accuse ten different product groups and thirteen different product combinations. More than two dozen witnesses spread across more than ten states, India, and the Czech Republic are expected to testify and there will be several hundred trial exhibits and thousands of pages of expert reports.

Even assuming this case does proceed by videoconference, this case will involve confidential and proprietary Cisco information and only a secure videoconferencing platform should be used. The Zoom videoconferencing platform has serious and verified security flaws and it should not be used in this case. Indeed, various U.S. cyber intelligence and governmental agencies such as the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the Federal Risk and Authorization Security Agency, and the National Aeronautics Space Agency ("NASA") have all banned the use of at least the free or commercial versions of Zoom for government business. Some U.S. school districts (including Fairfax County, Virginia) and foreign governments have recently banned Zoom outright or discouraged its use. Accordingly, if the trial is to proceed by videoconference, the Court should use the Cisco WebEx videoconferencing solution or another alternative to Zoom such as Google.

As for the unrelated transcript from the Centripetal/Keysight case, Cisco respectfully submits that the transcript is not relevant or helpful here because that case involved different products from a different company and almost entirely different patent claims. Moreover, that case settled mid-trial before Keysight put on any evidence to rebut Centripetal's case-in-chief. Accordingly, Cisco respectfully objects to the Court's consultation or reliance on the Keysight transcript or acceptance of it into evidence in this case, for the reasons stated herein and also for the reasons stated in Cisco's Motion in Limine No. 1. Cisco further submits that the technology tutorial that the Court has requested here will be an extremely useful resource for educating the Court on the technology at issue and all that is necessary for this purpose.

I. Motion to Forgo Trial Entirely by Videoconference

Pursuant to Federal Rule of Civil Procedure 43(a), Cisco respectfully moves the Court to forgo trial entirely by videoconference and reset trial for a time when the parties can safely present their witnesses and evidence live and in person. In the alternative, to the extent trial will proceed by videoconference, Cisco respectfully moves the Court to select a secure videoconferencing platform that will enable the parties to protect confidential and proprietary information that will be presented at trial.

This is a complex patent case and trial exclusively by video here will be unwieldy and will unavoidably and unfairly prejudice Cisco's ability to cross-examine Centripetal's witnesses and the Court's ability to assess witness demeanor. This five-patent case is far-ranging and complex, and will include numerous fact and expert witnesses presenting complex testimony and evidence. In addition, the parties anticipate that certain witnesses will contradict others, which will require the Court (as the finder of fact) to make a multitude of credibility determinations. To Cisco's knowledge, no matter of this case's complexity has ever been tried entirely by videoconference and there is no reason to make this case the first. To the contrary, this matter

can safely and conveniently be reset for a time when live proceedings can safely proceed. Nor will plaintiff suffer any material prejudice by such a delay—indeed, Centripetal itself originally proposed trial in this matter to conclude in September 2020, and Cisco is aware of no COVID-19 projections under which the Court would need to remain closed so long as to push proceedings beyond that date. No compelling circumstances warrant limiting the parties to video evidence here, when every indication is that a trial "in open court" as Rule 43(a) provides and encourages will be possible mere months from now.

The Court also expressed a concern that this matter may involve issues of national security that make trial more urgent. Tr. of Teleconf. Proceedings (Apr. 8, 2020) at 19. But unlike Cisco, which supplies a significant portion of the U.S. national security infrastructure, Centripetal has never sold any security products to the Department of Defense. There is nothing about Centripetal's business or its publicly available patents that will implicate matters of national security, and the timing of trial also will have no impact on national security.

A. Factual and Procedural Background

Despite Centripetal's request to try this case in September 2020 (*see* Tr. of Proceedings (Sept. 11, 2019) at 5), the Court set this case for a jury trial beginning April 7, 2020. Responding to concerns posed by the COVID-19 pandemic, the parties waived their respective jury demands and the Court scheduled this case for an in-person bench trial beginning May 6, 2020. *See* Tr. of Teleconf. Proceedings (Mar. 12, 2020). On April 8, 2020, the Court held a further teleconference and indicated that the bench trial would proceed as scheduled but be conducted entirely by remote videoconferencing. *See* Tr. of Teleconf. Proceedings (Apr. 8, 2020) at 2; *see also* Dkt. 367 at 1. The Court also indicated that it would use the Zoom videoconferencing platform, unless counsel provides "a good reason" not to use Zoom. *See* Tr. of Teleconf. Proceedings (Apr. 8, 2020) at 10. As stated on the teleconference, Cisco objects to conducting

the trial by videoconference, and to using the Zoom platform for any such proceeding. *Id.* at 14–15.

B. Argument

Federal Rule of Civil Procedure 43(a) provides that, "[a]t trial, the witnesses' testimony must be taken in open court unless a federal statute, the Federal Rules of Evidence, these rules, or other rules adopted by the Supreme Court provide otherwise." Fed. R. Civ. P. 43(a) (emphasis added). Cisco knows of no statute or rule providing for an entire trial by videoconference in the context of a case of this complexity, nor does Rule 43(a) suggest or contemplate that an entire complex patent case can be tried from start to finish pursuant to this Rule. Instead, Rule 43(a) provides that, "[f]or good cause in compelling circumstances and with appropriate safeguards, the court may permit testimony in open court by contemporaneous transmission from a different location." *Id.* But there is no good cause and no compelling circumstances justifying holding an entire complex trial of this magnitude in this case in May, when all indications are that the in-person trial the Rule contemplates will be possible a few months hence. Rule 43(a)'s narrow exception to the underlying requirement that trial occur in open court typically applies to permit remote testimony from select witnesses who cannot attend trial due to "accident or illness," "would be endangered or made uncomfortable by appearing in a courtroom," or are located faraway. *Eller v. Trans Union, LLC*, 739 F.3d 467, 478 (10th Cir. 2013) (collecting cases).

This patent case should not be the first case of this complexity tried entirely by video. Although the COVID-19 pandemic is certainly good cause to delay trial until it can safely proceed in-person, there are no compelling circumstances that require proceeding with video technology on May 6 as opposed to providing the parties with their "day in Court" as soon as it is safe to do so.

1. Compelling Cisco to Try This Case Entirely By Videoconference Is Unfair and Unnecessary

a. Trial by Videoconference Will Unfairly and Prejudicially Confine Cisco's Ability to Present Its Case and Cross-Examine Witnesses, As Well As the Court's Ability to Evaluate Witness Demeanor

Courts, including the Fourth Circuit, have recognized that trial testimony taken by videoconference poses challenges in evaluating the credibility and persuasiveness of witnesses, as well as performing cross-examination. *See, e.g.*, *Rusu v. U.S. I.N.S.*, 296 F.3d 316, 322 (4th Cir. 2002) ("[V]ideo conferencing may render it difficult for a factfinder in adjudicative proceedings to make credibility determinations and to gauge demeanor."); *Teller v. Helbrans*, No. 19-cv-3172, 2019 WL 3975555, at *2 (E.D.N.Y. Aug. 21, 2019) (Bulsara, M.J.) ("[C]onducting cross-examination at a trial via video of a party is near impossible, unless Petitioner is given full advance notice of all documents to be used during such an inquiry. That is highly unorthodox and threatens to prejudice Respondent."). Thus remote testimony is permitted only with "safeguards" that are "appropriate" in light of the relevant witness's testimony and evidence. *See, e.g.*, *Niemeyer v. Ford Motor Co.*, No. 09-cv-2091, 2012 WL 5199145, at *3 (D. Nev. Oct. 18, 2012) (noting that "Rule 43(a) requires 'appropriate safeguards' and none have been provided," where "testimony via video transmission will severely impede defendants' ability to cross examine a medical witness using important documentary evidence and medical records").

Here, the complexity and nature of the allegations in this case will prevent an adequate presentation of the accused technologies and complicated issues at stake. This is not a simple dispute. It involves five patents, ten different accused product groups, and thirteen different accused product combinations, along with more than two dozen fact witnesses and experts located across more than ten states, thousands of pages of expert reports, and what will likely be

several hundred trial exhibits. *See* Cisco's Mem. in Support of Mot. to Bifurcate, Dkt. 252 at 3–9 (describing breadth and complexity of case). Moreover, Centripetal seeks almost $500 million in damages and has made very serious (although ultimately baseless) allegations that Cisco copied Centripetal's technology—allegations that Cisco intends to disprove at trial, but that will require intricate and detailed affirmative testimony and cross-examination.

The complexity and length of a trial by videoconference here would unfairly prejudice Cisco's ability to present its case and the Court's ability to evaluate it. The Court would be required to assess the demeanor and candor of numerous witnesses—many of whom it has never met before—from afar. In this case, it will be especially important for the Court to assess the credibility of Centripetal's witnesses who allege that Cisco copied Centripetal's technology, as well as Cisco's witnesses who actually developed the accused technology and will vigorously rebut Centripetal's copying accusations. Cisco's ability to cross-examine Centripetal's witnesses, and the Court's ability to discern who is credible and who is speculating, are prejudicially diminished in this case when witness, questioner, and factfinder are only connected by a video feed. Many critically important physical and emotional cues will be lost from the lack of in-person interaction and the nature of the video feed, which likely will be nothing more than video shot of a person's head. *See* Fed. R. Civ. P. 43 advisory committee's note (1996 amendment) ("The importance of presenting live testimony in court cannot be forgotten. The very ceremony of trial and the presence of the factfinder may exert a powerful force for truthtelling. The opportunity to judge the demeanor of a witness face-to-face is accorded great value in our tradition."); *United States v. Lawrence*, 248 F.3d 300, 304 (4th Cir. 2001) ("[V]irtual reality is rarely a substitute for actual presence and . . . even in an age of advancing

technology, watching an event on the screen remains less than the complete equivalent of actually attending it.").

Trial of this case by videoconference will also necessarily limit Cisco's ability to effectively cross-examine witnesses. A witness facing cross-examination typically does not know in advance which documents will be used by the cross-examining attorney. As far as Cisco is aware, a trial by videoconference would require sending documents to be used on cross to the witness and counsel in advance. Indeed, in the parties' current exchange on the draft Pretrial Order, this is the very proposal Centripetal is making. But that early notice of documents provides a "road map" to the adverse witness, thereby diminishing the effectiveness of the cross-examination. *See Teller*, 2019 WL 3975555, at *2 ("[C]onducting cross-examination at a trial via video of a party is near impossible, unless Petitioner is given full advance notice of all documents to be used during such an inquiry. That is highly unorthodox and threatens to prejudice Respondent."). The only safeguard that could remedy this prejudice would be to require that only electronic versions of cross-examination exhibits be sent to the adverse witness one-by-one as introduced.

A trial by videoconference, coupled with audio availability to the public, also eliminates the ability to police the Rule of Sequestration, under Federal Rule of Evidence 615, which Cisco intends to invoke in light of the unfounded allegations of copying being made by Centripetal here. When "the Rule" is invoked in a typical courtroom setting, witnesses are either present or not present in the Court, with counsel for both sides monitoring courtroom observers for compliance. A videoconference trial has no such adequate safeguard to protect the integrity of the process.

Moreover, the quality of the video feed on any videoconferencing platform inevitably will fluctuate depending on, *inter alia*, the strength and stability of the Court's, witnesses' and parties' internet connections (which can fluctuate outside of their control for any number of reasons, including the number of internet users in a geographic area at any given point in time). The unique circumstances of the present day, with many witnesses potentially appearing from their homes rather than more infrastructure-robust professional settings, pose a particular challenge: even with the highest quality internet services available for in-home use, internet bandwidth and related issues can occur in any given home during the trial day because of the household demands from family needing internet for remote schooling for their children, dual-income families who must also be working remotely during the entire trial day, and the simple periodic glitches that are routine with daily Internet use across a provider's network—which is only exacerbated with nearly the entire country working or learning remotely during the pandemic. With respect to this particular trial, the number of participants logged into the selected videoconferencing platform, as well as the various types of cameras, microphones, computers, monitors and other technology available to witnesses and others, will only increase the likelihood of technological failures.

b. There Are No Compelling Circumstances to Conduct an Unprecedented Trial by Videoconference Here

Rule 43(a) also requires "compelling circumstances" to permit a remote witness's testimony at trial. Fed. R. Civ. P. 43(a). There are no such circumstances (and Centripetal has not identified any) here dictating that trial must proceed on May 6 by videoconference as to any witness, instead of at a later date "in open court" as Rule 43(a) envisions. Indeed, Centripetal itself originally proposed trial in September 2020. *See* Tr. of Proceedings (Sept. 11, 2019) at 5.

The Court mentioned the issue of national security as a one of the factors that warranted maintaining the May trial date. Tr. of Teleconf. Proceedings (Apr. 8, 2020) at 19. Cisco expects that the Court's recollection of this issue is tied to a previous assertion by Centripetal's counsel that its patented technology was developed in connection with the U.S. military and with the goal of helping the government. To be clear, whatever motivated Centripetal to get into the security business, this case, or the timing of trial will have no impact on national security. For example, Jonathon Rogers (Centripetal's COO and corporate representative during the Keysight trial) testified that Centripetal has never sold products to the Department of Defense. Rogers Dep. (Dec. 10, 2019) at 56:17-19. Likewise, Mr. Rogers made clear that despite the military background of several founders of Centripetal, its technology did not come from military secrets. *Id.* at 48:19-25.[1] Accordingly, there is no reason relating to "national security" why the trial must go forward in May, and certainly not a compelling circumstance warranting deviation from Rule 43(a)'s requirement that testimony ordinarily be taken "in open court."

Instead, there are compelling reasons not to conduct an unprecedented trial by videoconference during this time. Because of the COVID-19 pandemic, virtually all of the attorneys and witnesses in this case are under stay-at-home orders and thus unable to meet in person. Although videoconferencing technology can certainly facilitate communication between attorneys and witnesses, it is not a substitute for intensive, face-to-face preparation required for a trial of this magnitude and complexity. *Cf. United States v. Davis*, No. ELH-20-09, 2020 WL 1529158, at *7 (D. Md. Mar. 30, 2020) (noting that Zoom "is no substitute for a face-to-face, in

[1] In contrast, Cisco's security products have been sold to the U.S. government for many years now, including long before Centripetal accused it of infringement. These includes sales to the Department of Defense, every branch of the military, various intelligence and law enforcement agencies, and the Federal courts, among others.

(continued)

person, contact meeting between an attorney and his client").[2] Further, the Court indicated in the April 8 hearing that it might limit the number of lawyers who have access to the video feed for this trial. With attorneys under stay-at-home orders, this further restriction means, in effect, that key members of both parties' legal teams, including in-house counsel responsible for this matter, may not have access to the trial. This type of restriction would never be imposed in a case proceeding in open Court. The only practical workaround to ensure that Cisco's trial team puts its best foot forward on behalf of its client is for Cisco's in-house counsel and outside attorneys to congregate in one place to view the video feed and work as a coherent trial team, in violation of recommended CDC guidelines on social distancing.

To Cisco's knowledge, no court in this District has denied, and no party has opposed, a motion for continuance of trial based on COVID-19 concerns.[3] This case is not an emergency,

[2] In this regard, a trial by videoconference here would be even worse than the "Catch 22" situation described by the Fourth Circuit in the immigration context, where hearings are sometimes held remotely. Because of stay-at-home orders, counsel cannot even choose between being present with their witnesses versus being present in the courtroom with the factfinder and opposing counsel—witness, factfinder, and opposing counsel will all be in different places. Thus, the parties will be prejudiced in their ability to advocate effectively no matter how they choose to prepare and present their case. *See Rusu*, 296 F.3d at 323 (noting "Catch 22" situation posed by videoconferencing, where attorney must choose between being able to "confer privately and personally assist in the presentation of the client's testimony" and interacting "effectively" with the Court and opposing counsel).

[3] A recent decision by a Minnesota district court only serves to illustrate that there are no similarly compelling circumstances warranting a trial by videoconference here. In that decision, the court ordered the last two days of a thirteen-day bench trial to be completed by three-way video feed between the Minnesota courthouse and two other courthouses local to the two remaining defendants' witnesses. *In re RFC & ResCap Liquidating Tr. Action*, No. 13-cv-3451, 2020 WL 1280931, at *4 (D. Minn. Mar. 13, 2020). The two remaining witnesses were examined by attorneys from both parties in person at the latter two courthouses. *See id.* The court noted that delaying the last two days of trial would prejudice plaintiff by giving defendants "an additional seven to eight weeks to prepare their damages expert." *Id.* Here, in contrast, trial has not yet begun so a postponement would not disrupt any ongoing proceedings and would affect both parties' preparation equally.

nor will Centripetal suffer any cognizable prejudice by waiting until a trial may safely be held in person, as Rule 43(a) envisions.

2. If the Court Proceeds with Trial by Videoconference, It Should Not Use Zoom, Which is Unsecure and Poses Grave Security Risks

This Court has indicated that it intends to use the Zoom videoconferencing platform to host this trial, unless counsel provides "a good reason" not to use Zoom. *See* Tr. of Teleconf. Proceedings (Apr. 8, 2020) at 10. Cisco respectfully submits that the choice of Zoom poses security risks that cannot be remedied by any appropriate safeguards.

Just in the past few weeks, Zoom has come under increasing scrutiny by law enforcement, government agencies, schools, cybersecurity professionals, and other institutions for issues relating to, *inter alia*, routing U.S. and Canada meetings and data to China, using encryption keys located in China (which can be demanded by the Chinese government under Chinese law), using outdated encryption key standards, claiming to offer end-to-end encryption but now admitting that they do not have such encryption ("Currently, it is not possible to enable E2E encryption for Zoom meetings" according to a Zoom spokesperson), illegally sharing user and personal data, leaks of users' personal data, security vulnerabilities that allowed malicious actors to access and control microphones and cameras and gain root access to MacOS laptops, undisclosed data collection and sharing practices, and "Zoombombing" (i.e., harassment during Zoom sessions, allegedly even those protected by password, by hackers and other intruders).[4]

[4] *See, e.g.*, Rae Hodge, *Zoom: Every Security Issue Uncovered in the Video Chat App*, CNET (Apr. 8, 2020), https://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app; Zack Whittaker, *New York City Bans Zoom in Schools, Citing Security Concerns*, TechCrunch (Apr. 5, 2020), https://techcrunch.com/2020/04/05/zoom-new-york-city-schools; Aaron Tilley & Roert McMillan, *Zoom CEO: 'I Really Messed Up' on Security as Coronavirus Drove Video Tool's Appeal*, The Wall Street Journal (Apr. 4, 2020), https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129; Micah Lee, *Zoom's Encryption Is "Not Suited for Secrets"* (continued)

Indeed, Virginia is no exception: Zoombombing has disrupted a Norfolk school's online classes and reached other groups in the wider Virginia area, and public schools in Fairfax County have banned the use of Zoom.[5] Even meetings protected by password have allegedly been disrupted.[6]

Because of the various vulnerabilities and security flaws in the Zoom platform, the U.S. Senate, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the Federal Risk and Authorization Security Agency, NASA, various foreign governments or their agencies (e.g., the Taiwanese government, German Foreign Ministry, Australian Defense Force, Singapore Ministry of Education), and various companies (e.g., Google, SpaceX) have banned or strongly discouraged the use of at least the free or commercial versions of Zoom.[7] For example, the U.S. Sergeant at Arms reportedly warned Senate offices

---

and Has Surprising Links to China, Researchers Discover, The Intercept (Apr. 3, 2020), https://theintercept.com/2020/04/03/zooms-encryption-is-not-suited-for-secrets-and-has-surprising-links-to-china-researchers-discover/?source=techstories.org; Thomas Brewster, *Warning: Zoom Makes Encryption Keys in China (Sometimes)*, Forbes (Apr. 3, 2020), https://www.forbes.com/sites/thomasbrewster/2020/04/03/warning-zoom-sends-encryption-keys-to-china-sometimes/#337a56513fd9; Micah Lee & Yael Grauer, *Zoom Meetings Aren't End to End Encrypted, Despite Misleading Marketing*, The Intercept (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption.

[5] *See, e.g.*, Adrienne Mayfield, *Norfolk Zoom Class Hijacked, 'Inappropriate Materials' Shared with Students*, WFXR Fox (Mar. 31, 2020), https://www.wfxrtv.com/news/norfolk-zoom-class-hijacked-inappropriate-materials-shared-with-students; Taylor Lorenz & Davey Alba, *'Zoombombing' Becomes a Dangerous Organized Effort*, Boston.com (Apr. 3, 2020), https://www.boston.com/news/technology/2020/04/03/zoombombing-becomes-a-dangerous-organized-effort (noting that an online Zoombombing group "discussed disrupting a singles mixer organized by a Baptist church in Virginia"); Sara Morrison, *Zoom Responds to Its Privacy (and Porn) Problems*, Vox (Apr. 2, 2020) ("Public schools in Fairfax County, Virginia, for example, announced . . . that they 'can no longer use Zoom' for video calls.").

[6] *See, e.g.*, David DeBolt, *'Zoom Bomber' Exposed Himself to Berkeley High Students, School Official Says*, East Bay Times (Apr. 8, 2020), https://www.eastbaytimes.com/2020/04/08/zoom-bombers-disrupt-berkeley-schools.

[7] *See, e.g.*, Jalelah Abu Baker, *MOE Suspends Use of Zoom in Home-Based Learning Following Breaches Involving Obscene Images*, Channel News Asia (Apr. 10, 2020), https://www.channelnewsasia.com/news/singapore/moe-suspends-zoom-home-based-learning-
(continued)

last week that Zoom has been "issued a high-risk notice" and poses the threat of "potential compromise of systems and loss of data, interruptions during a conference, and lack of privacy."[8] Likewise, the Senate Rules Committee reportedly instructed Senate offices "to only use Senate-supported technologies," which do not include Zoom.[9] Indeed, government agencies throughout the United States—including the Department of Justice and the FBI (including the FBI Norfolk Field Office)—have issued recent warnings about the risks of using Zoom due to Zoombombing and other security issues.[10]

---

obscene-images-12626534; Kiran Stacey & Hannah Murphy, *US Senate Tells Members Not to Use Zoom*, Financial Times (Apr. 9, 2020), https://www.ft.com/content/dac7d60b-54fa-402b-8469-70f85aaace76; John Moreno, *Google Bans Employees from Using Zoom*, Forbes (Apr. 9, 2020), https://www.forbes.com/sites/johanmoreno/2020/04/09/google-bans-employees-from-using-zoom/#590fbdc1770f; Brandon Vigliarolo, *Who Has Banned Zoom? Google, NASA, and More*, TechRepublic (Apr. 9, 2020), https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more; *Zoom Banned by Taiwan's Government over China Security Fears*, BBC (Apr. 7, 2020), https://www.bbc.com/news/technology-52200507.

[8] Cristiano Lima, *Internal Senate Memo Warns Zoom Poses 'High Risk' to Privacy, Security*, Politico (Apr. 9, 2020), https://www.politico.com/news/2020/04/09/internal-senate-memo-warns-zoom-poses-high-risk-to-privacy-security-177347.

[9] *Id.*

[10] U.S. Dep't of Justice, *Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic* (Apr. 3, 2020), https://www.justice.gov/usao-edmi/pr/federal-state-and-local-law-enforcement-warn-against-teleconferencing-hacking-during; Adrienne Mayfield, *Norfolk Zoom Class Hijacked, 'Inappropriate Materials' Shared with Students*, WFXR Fox (Mar. 31, 2020), https://www.wfxrtv.com/news/norfolk-zoom-class-hijacked-inappropriate-materials-shared-with-students (noting guidance from the FBI Norfolk Field Office); Mairead McArdle, *New York Attorney General Examining Zoom Privacy Practices*, Nat'l Review (Mar. 31, 2020), https://www.nationalreview.com/news/new-york-attorney-general-examining-zoom-privacy-practices; Fed. Bureau of Investigation, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic* (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

(continued)

These same security flaws caution against using Zoom here.[11] This trial will involve discussion and transmission of sensitive Cisco source code, some of which is used in the computer systems of the United States military and other government institutions. The potential threat to national security by conducting this trial by Zoom cannot be overstated, especially when new Zoom-related risks are being made public every day. The rapidly evolving situation around Zoom suggests that there is no appropriate safeguard[12] that would minimize the possibility of a data breach should this trial be conducted on the Zoom platform. Thus, if the Court intends to

[11] It is Cisco's understanding that the premium versions of the Zoom videoconferencing platform, as well as the "Zoom for Government" version, do not resolve all of the security issues discussed above. At best, the premium versions appear to provide a Zoom host with greater user management controls, which may help alleviate some instances of Zoombombing. But Cisco has found no indication in Zoom's own website or publicly available sources that the premium versions provide, e.g., a more secure method of storing or routing user data. *See, e.g.*, Zoom, *Zoom Meeting Plans for Your Business* (last visited Apr. 9, 2020), https://zoom.us/pricing (no mention of enhanced security features for premium versions); Michael Archambault, *How to Increase Your Privacy and Security in Zoom*, Digital Trends (Apr. 6, 2020), https://www.digitaltrends.com/computing/how-to-increase-your-privacy-security-zoom (no mention of upgrading to premium versions as a method for increasing the privacy or security of Zoom sessions). Similarly, Cisco has found no indication that the "Zoom for Government" version addresses the security flaws discussed above, except for possibly the issue of using encryption keys located in China. *See* Eric S. Yuan, *Response to Research from University of Toronto's Citizen Lab*, Zoom Blog (Apr. 3, 2020), https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab (noting that the "Zoom for Government cloud" was not affected by the China encryption keys issue).

[12] Several categories of information that will be offered into evidence at trial qualify as trade secrets or implicate governmental interests that overcome the public's presumptive right of access to the trial proceedings. In particular, Cisco's confidential source code, confidential financial and sales information and other confidential technical information should be sealed from public disclosure. *See e.g.*, *Eden Hannon & Co. v. Sumitomo Trust & Banking Co.*, 914 F.2d 556, 562 (4th Cir. 1990) (confidential financial information entitled to trade secret protection); *Lifenet Health v. Lifecell Corp.*, No. 13-cv-486, 2015 U.S. Dist. LEXIS 181315, at *6 (E.D. Va. Jan. 9, 2015) (trade secrets entitled to be sealed at trial include manufacturing processes); *ATI Indus. Automation, Inc. v. Applied Robotics, Inc.*, 801 F.Supp.2d 419, 425 (M.D.N.C. 2011) (private property interest in maintaining the secrecy of financial and sales information overcame the public's First Amendment right of access). Use of Zoom, however, poses a significant risk of public disclosure of this confidential information, regardless of any measures the Court may take to protect this information from disclosure.

proceed with a trial by videoconference—though Cisco maintains that it should not—it should employ a secure alternative option, such as Cisco's own WebEx product or Google. *See, e.g.*, Cisco, *Cisco WebEx Trusted Platform* (last visited Apr. 9, 2020), https://www.cisco.com/c/en/us/about/trust-center/webex.html (discussing WebEx's end-to-end encryption and other data protection and privacy features); Jonny Evans, *12 Zoom Alternatives for Secure Video Collaboration*, Computerworld (Apr. 6, 2020), https://www.computerworld.com/article/3536471/12-zoom-alternatives-for-secure-video-collaboration.html ("If security and privacy matter to your business, Webex Meetings offers end-to-end encryption as an option.").

II. Objection to Use of Transcript from Keysight Trial

The Court raised the possibility of reviewing the transcript from the Centripetal/Keysight case as a means for getting up to speed on the technology relevant to this case. Tr. of Teleconf. Proceedings (Apr. 9, 2020) at 4. Cisco respectfully submits that the technology tutorial that the Court has requested at the start of the trial will achieve this purpose. Cisco also respectfully submits that the Centripetal/Keysight transcript is not relevant or helpful for three reasons: (1) there is only minor overlap between the asserted patents from that case and this case (only one set of asserted claims overlaps); (2) there is no overlap regarding the types of accused products; and (3) the case settled mid-trial before Keysight put on any evidence to rebut Centripetal's case-in-chief. For the Court to review a one-sided record showcasing Centripetal's view of a different case, to which Cisco was not a party and accordingly had no role in shaping, would be unfairly prejudicial. Each issue is discussed below.

The Patents. The Keysight trial involved six patents,[13] two of which overlap with this case: the '205 Patent and the '856 Patent. Only two of the ten total patent claims asserted in this case—both from the '856 Patent—overlap with the Keysight trial. The '205 Patent, meanwhile, is the patent on which the PTAB instituted an IPR for 48 of its 96 claims, and those instituted claims remain subject to the Court's February 25, 2020 stay Order. And indeed, all 48 of those instituted claims have since been invalidated.

The Accused Products. As Centripetal's Vice President of Sales, Christopher Gibbs, confirmed, the Keysight/Ixia products at issue in the prior trial are different than the Cisco products at issue in this case. He would know because he was a former Cisco sales person that Centripetal hired away from Cisco. Gibbs Dep. (Dec. 17, 2019) at 14:11-13. Both Centripetal and Keysight sell what Centripetal refers to as a "threat intelligence gateway" product, but Cisco's products are different. According to Mr. Gibbs, Centripetal's threat intelligence gateway product is called RuleGate, and Keysight/Ixia's threat intelligence gateway product is called ThreatArmor. *Id.* at 13:7-12, 43:1-8. Mr. Gibbs testified that, as of the Keysight litigation, the Keysight/Ixia ThreatArmor product was Centripetal's primary competition in the threat intelligence gateway market. *Id.* at 42:17-23. Although Cisco's counsel twice asked Mr. Gibbs to identify any other companies in the threat intelligence gateway market, he listed only three other companies—none of which was Cisco. *Id.* at 44:2-44:6. Cisco's counsel then asked Mr. Gibbs about the products that are the center of this case, i.e., Cisco's "StealthWatch," encrypted traffic analytics ("ETA") product and its cognitive threat analytics ("CTA") product.

[13] The full patent numbers are: U.S. Patent Nos. 9,137,205 ("the "'205 Patent"), 9,560,077 ("the "'077 Patent"), 9,565,213 ("the "'213 Patent"), 9,413,722 ("the "'722 Patent"), 9,264,370 ("the "'370 Patent"), and 9,917,856 ("the "'856 Patent"). The '077 Patent and the '213 Patent have since been invalidated in their entirety through IPRs.

Notwithstanding his responsibilities of managing the revenue generation of Centripetal's offerings, Mr. Gibbs testified that he could not recall ever discussing Stealthwatch with a customer, and that he had never heard of the terms ETA or CTA. *Id.* at 8:12-15, 25:22-26:15. Accordingly, studying the Keysight trial will not inform the Court about the products accused in this case.

Finally, a review of the Centripetal/Keysight transcript provides the Court with only Centripetal's case-in-chief. Keysight put on no countering evidence and any of its case, because the case settled mid-trial. And of course, Cisco had no role in shaping the Keysight record at all, as it was not a party.

Accordingly, Cisco respectfully objects to the Court's consultation or reliance on the Keysight transcript or acceptance of it into evidence in this case, for the reasons stated herein and also for the reasons stated in Cisco's Motion in Limine No. 1. Cisco further submits that the technology tutorial that the Court has requested here will be an extremely useful resource for educating the Court on the technology at issue and all that is necessary for this purpose.

III. Conclusion

For the above reasons, the Court should not hold a trial entirely by videoconference and should reset trial for a time when the parties can safely present their witnesses and evidence live and in person. In the alternative, to the extent trial will proceed by videoconference, the Court should select a videoconferencing platform that will enable the parties to present confidential information securely. Finally, the Court should not consult or rely on the Keysight transcript, but rather should receive evidence and argument only from the parties to this case, including through the planned technology tutorial.

CISCO SYSTEMS, INC.

By /s/
Of Counsel

Dabney J. Carr, IV, VSB No. 28679
TROUTMAN SANDERS LLP
P. O. Box 1122
Richmond, Virginia 23218-1122
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
dabney.carr@troutmansanders.com

DAVIS POLK & WARDWELL LLP
Neil H. MacBride, VSB No. 79883
901 15th Street, NW
Washington, DC 20005
Tel: (202) 962-7000
Fax: (202) 962-7111
neil.macbride@davispolk.com

DUANE MORRIS LLP
Louis N. Jameson (admitted pro hac vice)
Matthew C. Gaudet (admitted pro hac vice)
John R. Gibson, VSB No. 72968
Jennifer H. Forte (admitted pro hac vice)
1075 Peachtree Street, N.E., Suite 2000
Atlanta, Georgia 30309-3929
Telephone: (404) 253-6900
Facsimile: (404) 253-6901
wjameson@duanemorris.com
jrgibson@duanemorris.com
jhforte@duanemorris.com

Joseph A. Powers (admitted pro hac vice)
30 South 17th Street
Philadelphia, PA 19103-4196
Telephone: (215) 979-1000
Facsimile: (215) 689-3797
japowers@duanemorris.com

John M. Baird, VSB No. 77827
Christopher J. Tyson, VSB No. 81553
505 9th Street, N.W., Suite 1000
Washington, DC 20004-2166
Telephone: (202) 776 7851
Facsimile: (202) 478 2620
jmbaird@duanemorrris.com

cjtyson@duanemorris.com

Nicole E. Grigg (formerly Johnson) (admitted *pro hac vice*)
2475 Hanover Street
Palo Alto, CA 94304-1194
Telephone: (650) 847-4176
Facsimile: (650) 618-2713
NEGrigg@duanemorris.com

Counsel for Defendant Cisco Systems, Inc.