

2020-1635, 20-1636

United States Court of Appeals for the Federal Circuit

Centripetal Networks, Inc.,
Appellant,

v.

Cisco Systems, Inc.,
Appellee.

Appeals from the United States Patent and Trademark Office, Patent Trial and
Appeal Board in Nos. IPR2018-01436 and IPR2018-01437

OPENING BRIEF FOR APPELLANT CENTRIPETAL NETWORKS, INC.

Paul J. Andre
James Hannah
KRAMER LEVIN NAFTALIS &
FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700

Jeffrey Price
KRAMER LEVIN NAFTALIS &
FRANKEL LLP
1177 Avenue of the Americas
New York, NY 10036
Telephone: (212) 715-7502

ATTORNEYS FOR CENTRIPETAL NETWORKS, INC.

CERTIFICATE OF INTEREST

Counsel for Appellant Centripetal Networks, Inc. certifies the following:

1. The full name of every party represented by us is:

Centripetal Networks, Inc.

2. The name of the real party in interest represented by us is:

Centripetal Networks, Inc.

3. All parent corporations and any other publicly held companies that own 10 percent or more of the stock of the party:

None

4. The names of all law firms and the partners or associates that appeared for Centripetal Networks, Inc. before the Patent Trial and Appeal Board or are expected to appear in this court (and who have not or will not enter an appearance in this case) are:

Paul Andre, Jeffrey Price, and James Hannah of Kramer Levin
Naftalis & Frankel LLP.

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal:

- *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, Case No. 2:18-cv-00094-HCM-LRL (E.D. Va.)

Dated: July 10, 2020

/s/ James Hannah

Paul J. Andre
James Hannah
Kramer Levin Naftalis & Frankel LLP
990 Marsh Road
Menlo Park, California 94025
Tel: (650) 752-1700
Fax: (650) 752-1800
pandre@kramerlevin.com
jhannah@kramerlevin.com

Jeffrey H. Price
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, NY 10036
Tel: 212.715.7502
Fax: 212.715.8302
jprice@kramerlevin.com

Attorneys for Appellant
Centripetal Networks, Inc.

TABLE OF CONTENTS

	<u>Page</u>
Statement of Related Cases.....	iv
Jurisdiction	1
I. Statement of the Issues	2
II. Statement of the Case and Facts	3
A. Centripetal’s Inventions	3
B. Sourcefire	6
C. The Final Written Decisions	7
1. Public Accessibility of Sourcefire	8
2. Patentability of the Challenged Claims Over Sourcefire	9
III. Summary of the Argument	13
IV. Standard of Review.....	15
V. Argument	15
A. Sourcefire is Not a Printed Publication.....	15
B. Sourcefire Does Not Render the Challenged Claims Obvious	21
1. Sourcefire Does Not Determine Whether a Packet Includes a Specified TLS-Version Value	21
2. Petitioner Did Not Demonstrate Any Motivation to Modify Sourcefire, But Instead Used Hindsight to Fill-In Missing Elements.....	24
C. Sourcefire Does Not Disclose the Claimed Operator	31
VI. Conclusion	34

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Acceleration Bay, LLC v. Activision Blizzard Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	16, 19, 20
<i>Arendi S.A.R.L. v. Apple Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016)	14, 25, 26
<i>Blue Calypso, LLC v. Groupon, Inc.</i> , 815 F.3d 1331 (Fed. Cir. 2016)	15
<i>Cisco Sys., Inc. v. Centripetal Networks, Inc.</i> , No. IPR2018-01760, 2019 WL 2180053 (P.T.A.B. May 20, 2019)	8
<i>In re Cronyn</i> , 890 F.2d 1158 (Fed. Cir. 1989)	15
<i>Dell Inc. v. Acceleron, LLC</i> , 884 F.3d 1364 (Fed. Cir. 2018)	19
<i>Fox Factory, Inc. v. SRAM, LLC</i> , 944 F.3d 1366 (Fed. Cir. 2019)	29, 30, 33
<i>Game & Tech. Co. v. Activision Blizzard Inc.</i> , 926 F.3d 1370 (Fed. Cir. 2019)	13, 24
<i>In re Hall</i> , 781 F.2d 897 (Fed. Cir. 1986)	16
<i>Icon Health & Fitness, Inc. v. Strava, Inc.</i> , 849 F.3d 1034 (Fed. Cir. 2017)	34
<i>Jazz Pharms., Inc. v. Amneal Pharms., LLC</i> , 895 F.3d 1347 (Fed. Cir. 2018)	15, 17
<i>In re Klopfenstein</i> , 380 F.3d 1345 (Fed. Cir. 2004)	18
<i>Mass. Inst. Of Tech. v. AB Fortia</i> , 774 F.2d 1104 (Fed. Cir. 1985)	18, 19

<i>Medtronic, Inc. v. Barry</i> , 891 F.3d 1368 (Fed. Cir. 2018)	19, 20
<i>Merck & Cie v. Gnosis S.p.A.</i> , 808 F.3d 829 (Fed. Cir. 2015)	15
<i>In re NuVasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016)	33
<i>Rovalma, S.A. v. Bohler-Edelstahl GmbH</i> , 856 F.3d 1019 (Fed. Cir. 2017)	15
<i>Samsung Elecs. Co. v. Infobridge Pte. Ltd.</i> , 929 F. 3d 1363 (Fed. Cir. 2019)	18
Statutes	
28 U.S.C. § 1295(a)(4)(A)	1
35 U.S.C.	
§ 102(b)	16
§ 103(a)	3

STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5, Centripetal Networks, Inc., states that:

(1) no appeal other than the current appeal has been taken in or from the United States Patent and Trademark Office, Patent Trial and Appeal Board's decisions in Case Nos. IPR2018-01436 and IPR2018-01437;

(2) Centripetal Networks, Inc., and Cisco Systems, Inc., are parties to *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, 2:18-cv-00094 (E.D. Va.); and

(3) no other cases may be directly affected by the Court's decision in this appeal.

JURISDICTION

The Patent Trial and Appeal Board (the “Board”) issued Final Written Decisions in IPR2018-01436 and IPR2018-01437 on January 23, 2020. Appx1-72; Appx73-108. Patent Owner, Centripetal Networks, Inc., timely filed a Notices of Appeal on March 24, 2020. Appx852–856; Appx7762–7766. This Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(4)(A).

I. STATEMENT OF THE ISSUES

1. Is a prior art reference publicly accessible when it is only made available to customers who paid over \$25,000 to obtain it?
2. Did the Board err in finding the Petitioner was not required to show a motivation to modify Sourcefire to read on a missing claim element while ignoring un rebutted objective indicia demonstrating that the modification was non-obvious?
3. Did the Board err in finding Sourcefire to teach the claimed “operator” where it adopted, without analysis, Petitioner’s bare assertion that the element is in Sourcefire while explicit contrary evidence?

II. STATEMENT OF THE CASE AND FACTS

This consolidated appeal is taken from an *inter partes* reviews of U.S. Patent Nos. 9,124,552 (the “’552 Patent”) and 9,160,713 (the “’713 Patent”), owned by Centripetal, in Case Nos. IPR2018-01436 and IPR2018-01437, respectively. Centripetal appeals the Board’s rulings that claims 1–21 of the ’552 Patent and claims 1–20 of the ’713 Patent are unpatentable under 35 U.S.C. § 103(a) (pre-AIA) over “Sourcefire 3D System User Guide” (“Sourcefire”). The ’713 Patent is a continuation of the ’552 Patent, and the two Patents share a specification. See Appx154 at 1:6–11. Unless otherwise specified, this Brief cites the ’552 Patent and the papers and exhibits filed in Case No. IPR2018-01436.

A. Centripetal’s Inventions

Centripetal is a cyber-security company based in Herndon, Virginia that develops and sells the RuleGATE and CleanINTERNET suite of products and services which protect a network against a variety of attacks. Based on over a decade of research, Centripetal was awarded the ’552 and ’713 Patents, which disclose exemplary techniques for preventing “[a] category of cyber attack known as exfiltrations.” Appx140 at 1:15–16. An exfiltration is an attack where a criminal gains access to a network and leaks sensitive information out of the network. *Id.* For example, a criminal may gain access to the network of a large corporation, like Target, and send out the personal information of Target’s customers, such as their

credit card information, home address, phone number, etc., to various servers on the Internet so that the information can be sold on the black market.

Information travels over the Internet using a variety of protocols, including TCP/IP. At a fundamental level, applications installed on computer exchange “messages,” which the TCP/IP protocol breaks down into small units of data called packets. Appx439–441; Appx6811; Appx6823–6827; Appx6682–6684, ¶ 47. These packets are sent over the Internet and reassembled at their destination. *Id.* For example, when a user of one computer requests a photo that exists on a server, the photo will be broken down into packets, sent through the Internet, and reassembled at the destination computer so that it can be viewed.

In order to hide their tracks, criminals in increasingly (and alarming) rates use encryption to exfiltrate information from a network. Encrypted traffic on the Internet often uses two protocols: “HTTPS,” which stands for “Hypertext Transfer Protocol Secure,” and “TLS,” which stands for “Transport Layer Security.” Appx143 at 7:53–60. Using these protocols, attackers disguise the exfiltrated information to hide the fact that sensitive information is leaving the network. Compounding this issue, early versions of TLS had vulnerabilities that allowed third-party decryption of encrypted communications.

Traditional security tools, like Sourcefire, reconstruct encrypted Internet traffic in order to make security decisions on whether the traffic should be allowed

or not. Appx442–446 (discussing traditional, stateful IPS systems like Sourcefire). Using the photo example, these traditional security tools will intercept and collect all of the packets of photo before sending the packets to the destination. If the photo is benign, the security tool will break the photo back down into packets and forward the packets to their destination. For encrypted data, the process is even more onerous because all of the packets must be reassembled, the content must be decrypted and analyzed, and if safe, re-encrypted and broken down into packets before being sent to its destination. Appx443.

The ‘552 and ‘713 Patents provide security for encrypted traffic in a different way. Instead of collecting and reconstructing the packets, the ‘552 and ‘713 Patents act as “packet filters,” which make security decisions based on data (*e.g.* a TLS-version value) located in individual packets. Appx442. Continuing the photo example, rather than reconstructing the photo to see if it is safe or not, the ‘552 and ‘713 Patents determine whether individual packets that make up the photo include data that violates any security rules. In this way, the ‘552 and ‘713 Patents avoid the computationally expensive process of reconstructing and deconstructing Internet communications. For encrypted traffic, the benefits are even greater because the ‘552 and ‘713 Patents avoid having to further decrypt and encrypt the data.

One method of determining whether a packet should be blocked or allowed using the technology of the ‘552 and ‘713 Patents involves applying an “operator” that specifies a “packet transformation function” to received packets. According to the claims of the ‘552 and ‘713 Patents, the operator specifies one or more TLS-values as well as a packet-transformation function (*e.g.* block or allow), as shown in these examples:

HTTP-EXFIL Operator	REQUIRE-TLS-1.1-1.2 Operator
<pre>Operator HTTP-EXFIL(ip-packet): Inspect app-pkt(ip-packet) match GET return ALLOW; Inspect app-pkt(ip-packet) match POST return BLOCK; Inspect app-pkt(ip-packet) match PUT return BLOCK; Inspect app-pkt(ip-packet) match DELETE return BLOCK; Inspect app-pkt(ip-packet) match CONNECT return BLOCK; Return BLOCK; End Operator HTTP-EXFIL;</pre>	<pre>Operator REQUIRE-TLS-1.1-1.2(ip-packet): Inspect app-pkt(ip-packet) match 1.0 return BLOCK; Inspect app-pkt(ip-packet) match 1.1 return ALLOW; Inspect app-pkt(ip-packet) match 1.2 return ALLOW; Return BLOCK; End Operator REQUIRE-TLS-1.1-1.2;</pre>

Appx143 at 7:31–38 and 7:64–8:6. Using this operator, rules can specify different packet transformation functions for different TLS-version values (*e.g.* BLOCK TLS 1.0 and ALLOW TLS 1.1), which is not possible using Sourcefire.

B. Sourcefire

Sourcefire is a user manual for the Sourcefire 3D System which is a traditional security tool which must reconstruct encrypted traffic in order to make security decisions. Appx2064-2065; Appx6607 at 121:21–123:9; Appx443 (citing Appx3668 at 3:60–65). Undisputed evidence demonstrates that Sourcefire was maintained on a password protected support website and only provided to customers of the corresponding Sourcefire 3D System, which cost over \$25,000.

Appx192; Appx554–558; Appx4695-4699; Appx4700-4702. There is no evidence in the record that Sourcefire was or would have been made available to interested members of the public upon request or that it could have been obtained by a person interested in the art via any other method, whether or not exercising reasonable diligence.

Rather than determining whether or not individual packets include information that violates a packet-filtering rule, as recited in the challenged claims, Sourcefire uses the traditional technique of TCP packet reassembly. Appx2064–2065; Appx6607 at 121:21–123:9; Appx443 (citing Appx3668 at 3:60–65). As set forth in the Sourcefire manual itself, the device “collects and reassembles all the packets that are part of a TCP session[, which]... allows the rules engine **to inspect the stream as a single, reassembled entity rather than inspecting only the individual packets that are part of a given stream.**” Appx2064-2065 (emphasis added). Given this technique, Sourcefire never makes a determination that any packets include specified TLS-version values. *Id.*; *see also* Appx145-147 at claims 1, 8, and 15; Appx159-160 at 1, 8, and 15.

C. The Final Written Decisions

On May 23, 2019, the Board entered Final Written Decisions finding that Sourcefire qualifies as a publically available printed publication and that each claim of the ’552 and ’713 Patents were unpatentable over Sourcefire, despite the

fact that Sourcefire was not available to the public and operates in a fundamentally different way than the ‘552 and ‘713 Patents. *See generally* Appx1–72, Appx73–107.

1. Public Accessibility of Sourcefire

The Board began its analysis contending with the question of whether or not Sourcefire qualifies as a printed publication. Appx19–31. Petitioner asserted two independent bases for the premise that Sourcefire was publicly accessible: “(1) a copy was enclosed on documentation disks (CD-ROM/DVD) included with each Sourcefire 3D System product sold by Sourcefire, Inc., and (2) it was available ‘for download by persons who had received a login and password from Sourcefire, Inc. to its support website.’” Appx23. Petitioner’s second argument was explicitly rejected in a related case. *See Cisco Sys., Inc. v. Centripetal Networks, Inc.*, No. IPR2018-01760, 2019 WL 2180053, at *5 (P.T.A.B. May 20, 2019) (“We agree with Patent Owner that the evidence and argument presented in the Petition is insufficient to establish that Sourcefire was publicly accessible via the Sourcefire website). However, the Board declined to reach that argument in either Final Written Decision currently under appeal. Appx25.

Instead the Board focused solely on the first argument, stating that Petitioner proved “by a preponderance of the evidence that Sourcefire was ‘publicly accessible’ through distribution on CD-ROM disks with public sales of the

corresponding Sourcefire products for several reasons.” Appx25. In particular, the Board stated that it could not determine whether an interested artisan would have found a purchase price in excess of \$25,000 “too high to acquire Sourcefire by purchasing a Sourcefire 3D system product.” Appx31.

Setting aside that the document was only available to interested persons by spending a considerable sum on the corresponding product, that the document was kept of a password protected website, that there was no evidence that an interested member of the public could have requested or otherwise obtained a copy from Sourcefire, and that the sole public document mentioning Sourcefire disparaged the manual, the Board determined that Sourcefire qualified as a printed publication for the sole reason that it was distributed to “586 customers with no obligations of confidentiality and with expectations that the information could be shared for non-commercial use.” Appx31.

2. Patentability of the Challenged Claims Over Sourcefire

After its determination that Sourcefire qualified as a printed publication, the Board considered the patentability of the challenged claims of the ’552 and ’713 Patents over Sourcefire, finding each claim unpatentable. Appx70; Appx105.

In both IPR2018-01436 and IPR2018-01437, the Board considered whether Sourcefire disclosed a determination of whether one or more received packets

include TLS-version values. The exact claim language from Claim 1 of each Patent follows:

responsive to **a determination** by the at least one processor **that one or more packets**, of the at least a portion of the plurality of HTTPS packets, **have one or more application-header-field values corresponding to one or more TLS-version values** of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations

Appx145 at Claim 1 (emphasis added).

a determination by the computing system that the first packet comprises data corresponding to a transport layer security (TLS)-version value

Appx159 at Claim 1.

The Board’s analysis started with a summary of Centripetal’s arguments, which noted that Sourcefire’s technique for filtering communications using TLS-version values does not meet the claims because Sourcefire only analyzes fully reconstructed messages rather determining whether any individual packet includes the specified TLS-version value, as recited in the claims. Appx42. This fundamental fact about Sourcefire’s operation is not in dispute and was, indeed, confirmed by Petitioner’s expert. *Id.* (citing Appx6606–6607 at 120:9–123:17).

The Board then restated Petitioner’s *non-sequitur* attorney argument, which is that the claims are not “limited to any specific method of determining a TLS version of any HTTPS packet.” Appx43 (citing Appx561). But whether or not the claims are “limited to any specific method,” the fundamental fact remains that

Sourcefire fails to disclose making **any** determination that a packet includes a specified TLS-version value by **any** method. See Appx600–605. Declining to address this fact head-on, the Board continued its analysis “assuming *arguendo* that Patent Owner is correct that Sourcefire discloses only obtaining TLS version information from reassembled handshake messages.” Appx47.

Instead of adhering to the unrebutted documentary and testimonial evidence in the record, the Board articulated its own reasoning allegedly supporting its finding “that Sourcefire still teaches a determination that a *packet* comprises TLS version information.” *Id.* The Board reached its conclusion based not on any argument or evidence of record, but on the (mistaken) basis that Centripetal agreed that Sourcefire analyzes individual packets in encrypted communications. Appx47-48 (citing Appx808 at 40:3–12). To the contrary, however, Centripetal explicitly **disagreed** with that very characterization of Sourcefire:

I dispute that, yes. And I think, this is where petitioner’s characterization of, you know, during his opening remarks he said that there’s no dispute that the data is extracted from a handshake packet in Sourcefire. We do dispute that. We’ve disputed that from the very first paper all through the last paper. It’s not extracted from a handshake packet; it’s extracted from a reconstructed handshake message. And so, there’s never a determination of what is in any one of those handshake packets, there’s no determination of what is in any one of the later https packets that might be received after the handshake.

Appx809-810 at 41:20-42:9; *see also* Appx808 at 40:3–20. Accordingly, the only argument or evidence supporting the Board’s determination that Sourcefire still

teaches a determination that a *packet* comprises TLS version information—Centripetal’s alleged admission that “Sourcefire teaches determining that the reassembled handshake message comprises TLS version data by extracting that data from the first packet of the message”—does not exist.

Based on this faulty premise, the Board then concluded that “[w]hether the system of Sourcefire itself recognizes that fact or deduces it is **irrelevant**; the relevant question is whether a *person of ordinary skill* would have been taught the recited determination (i.e., determining that a packet comprises TLS version data) based on Sourcefire and his/her own knowledge.” Appx48 (citing *In re Keller*, 642 F.2d 413, 425 (C.C.P.A. 1981)) (emphasis added). The Board never found, however, that Sourcefire actually discloses making the claimed determination or that it would have been obvious to modify Sourcefire’s technique to meet the challenged claims. *Id.*

With respect to the “operator” that specifies a “packet transformation function” element recited in the claims of the ’552 Patent, the Board adopted Petitioner’s attorney argument, supported only by a vague citation to ten pages of Sourcefire, that these elements are taught in the manual. Appx50–51 (“Based on the cited portions of Sourcefire, we agree with Petitioner.”). No such disclosure can be found in these ten pages, let alone in any other part of Sourcefire. See Appx2188–2197.

III. SUMMARY OF THE ARGUMENT

Sourcefire, the only reference cited against the claims, is not a publically accessible printed publication. The reference was maintained on a password protected website and was only made available to customers of the corresponding Sourcefire 3D system, which retailed for over \$25,000. Appx192; Appx4695, Appx4700. Petitioner did not argue, and the Board did not establish, that reasonable diligence extends to paying such a considerable sum for the right to access a user manual, which itself was publicly disparaged. Sourcefire was, therefore, not publicly accessible by interested persons in the art. Because Sourcefire is not a printed publication under the law, the Board's determination that the challenged claims are obvious must be reversed.

The Board also erred as a matter of law in finding that common sense could supply a limitation from the '552 and '713 Patent that is admittedly missing from Sourcefire—namely, a determination on a packet-by-packet basis that an individual packet includes a specified TLS-version value. Sourcefire undisputedly analyzes reassembled messages and never determines whether any individual packet includes the specified values. The Board's failure to consider whether a person of ordinary skill in the art ("POSA") would have modified Sourcefire to make such a determination—particularly in view of contrary objective indicia of non-obviousness—violates this Court's opinions in *Game & Tech. Co. v.*

Activision Blizzard Inc., 926 F.3d 1370, 1381 (Fed. Cir. 2019) and *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016).

Finally, the Board’s determination that Sourcefire teaches the “operator” that specifies a “packet transformation function” element recited in each challenged claim of the ’552 Patent is not supported by substantial evidence. In particular, the Board accepted Petitioner’s attorney argument that the limitation was taught somewhere in a ten-page span of Sourcefire with no further analysis, while inexplicably declining to consider Centripetal’s citation to the document explaining why such a disclosure could not exist, violates the APA and cannot rise to the level of substantial evidence.

In view of the foregoing, the Board’s decision finding the challenged claims of the ’552 and ’713 Patents obvious over Sourcefire must be reversed.

IV. STANDARD OF REVIEW

This Court reviews the Board’s decisions under the Administrative Procedure Act (“APA”). *See, e.g., Rovalma, S.A. v. Bohler-Edelstahl GmbH*, 856 F.3d 1019, 1024 (Fed. Cir. 2017). This Court “review[s] the Board’s conclusions of law de novo and its findings of fact for substantial evidence.” *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1337 (Fed. Cir. 2016) (citations omitted). Obviousness is a question of law based on underlying findings of fact. *Merck & Cie v. Gnosis S.p.A.*, 808 F.3d 829, 833 (Fed. Cir. 2015) (citations omitted).

Whether a reference qualifies as a printed publication under § 102 is a legal conclusion based on underlying fact findings. *Jazz Pharms., Inc. v. Amneal Pharms., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018). Where no facts are in dispute, the question of whether a reference represents a “printed publication” is a question of law. *In re Cronyn*, 890 F.2d 1158, 1159 (Fed. Cir. 1989). Public accessibility is a question that is reviewed for substantial evidence. *Jazz Pharms.*, 895 F.3d at 1356. Petitioner has the burden of persuasion to prove that a reference is printed publication. *Id.*

V. ARGUMENT

A. Sourcefire is Not a Printed Publication

Sourcefire is not a printed publication because it was only made available to customers of the corresponding Sourcefire 3D System, which retailed for more

than \$25,000, thereby restricting access to interested persons exercising reasonable diligence. Appx4695-4699; Appx4700-4702. The document was otherwise kept under lock and key on a password protected website, which demonstrates Sourcefire, Inc.'s, intention to restrict access. Appx434-438; Appx192. Indeed, there is no record evidence that Sourcefire was ever made available to the general public or that any member of the interested public could have located Sourcefire without paying for the corresponding Sourcefire 3D System. The question on appeal is, therefore, whether a reference is publicly accessible when it is only made available to customers who are willing to pay over \$25,000 to obtain it. The answer must be no.

“Because there are many ways in which a reference may be disseminated to the interested public, ‘public accessibility’ has been called the touchstone in determining whether a reference constitutes a ‘printed publication’ bar under 35 U.S.C. § 102(b).” *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986) (citations omitted). Public accessibility turns on whether the reference was “disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.” *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 772 (Fed. Cir. 2018).

As an initial matter, the Board erred as a matter of law by placing the burden of persuasion on Centripetal to “present... evidence as to whether an interested artisan would, or would not, have found the cost too high to acquire Sourcefire by purchasing a Sourcefire 3D system product.” Appx31. To the contrary, the burden of persuasion was always on Petitioner to prove that persons interested in the art could have located Sourcefire exercising reasonable diligence, including whether reasonable diligence extended to paying over \$25,000 to access the document. *Jazz Pharms.*, 895 F.3d at 1356. Instead of attempting to meet its burden to prove that an interested person would have spent over \$25,000 to access the user manual, however, Petitioner argued that “cost is **irrelevant** to whether Sourcefire is a printed publication.” Appx556 (emphasis added). But because purchase of the Sourcefire 3D System was the only way for a person to access Sourcefire, the burden was squarely on Petitioner to demonstrate that paying such a sum would have been considered reasonable diligence. *Jazz Pharms.*, 895 F.3d at 1356.

Declining to address whether a person interested in the art could have located Sourcefire exercising reasonable diligence, Petitioner staked its entire argument on the incorrect legal premise that “[a]ctual distribution, like with Sourcefire, is often relied upon as a proxy for public accessibility and, in turn, a determination that a reference is a printed publication.” Appx555 (citing *In re Klopfenstein*, 380 F.3d 1345, 1349-50 (Fed. Cir. 2004)). That is, Petitioner only

argued that dissemination of the Sourcefire user manual via sales of the corresponding Sourcefire 3D System to **private parties** was sufficient to demonstrate **public** accessibility merely because customers received the manual. Appx552–553. This is not the law, and the cases and legal premises relied upon by Petitioner and the Board are readily distinguishable from the facts of this case.

The Board first relied on *Mass. Inst. Of Tech. v. AB Fortia*, 774 F.2d 1104, 1109 (Fed. Cir. 1985) (“MIT”) and *Klopfenstein*, 380 F.3d at 1349 that actual dissemination of Sourcefire “far exceeds the number of disclosures recognized under the relevant dissemination law for printed publications” allegedly because “dissemination of a conference paper to six persons rendered it a printed publication.” Appx26. But both Petitioner and the Board overstate the holdings of these cases because while “a limited distribution **can** make a work publicly accessible,” the mere fact of limited distribution does not render the work publicly accessible. *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F. 3d 1363, 1374 (Fed. Cir. 2019) (emphasis added).

Both *MIT* and *Klopfenstein* are distinguishable from this case on the basis that they involved the “free distribution of academic documents to conference and meeting attendees whose express purpose for attending the conference was to

hear lectures [sic] regarding those same documents.”¹ Appx595 (emphasis added). In these cases, therefore, it is indisputable that “persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, [could] locate” the references because the attendees paid to attend the conference precisely so that they could hear about and access those references. *Acceleration Bay*, 908 F.3d at 772. Further, key to the holding in *MIT* was the fact that “the copies were freely distributed to interested members of the public.” *Medtronic, Inc. v. Barry*, 891 F.3d 1368, 1381 (Fed. Cir. 2018). Sourcefire was **not** freely distributed to the public, and there is no evidence in the record that any person interested in the art did or would have paid in excess of \$25,000 simply to receive the Sourcefire user manual or that such an action would be considered within the realm of “reasonable diligence.”

Finally, the Board cited the lack of confidentiality provisions in the Sourcefire manual to find evidence of public accessibility. Appx29–31; *see also* Appx26. Petitioner waived this argument, having raised it for the first time at the Oral Hearing. *See Dell Inc. v. Acceleron, LLC*, 884 F.3d 1364, 1369 (Fed. Cir. 2018); Appx789–790 at 21:23–22:5; Appx821 at 53:21–25. Nevertheless, the Board’s reliance on *Medtronic*’s discussion of confidentiality provisions is

¹ In characterizing Centripetal’s argument, the Board cut off and declined to address the emphasized language, thus reframing the argument solely in terms of whether or not the references were “free.” Appx26.

inapposite. See Appx29–31. In *Medtronic*, this Court considered confidentiality obligations in determining whether “materials that are **distributed at meetings or conferences**” could be considered publicly accessible. *Medtronic*, 891 F.3d at 1382 (emphasis added). POSAs attend meetings and conferences in order to hear about and receive the materials discussed and distributed there whereas there is no record evidence that any POSA would have paid the \$25,000 price tag for the opportunity to read the Sourcefire user manual. *Medtronic* did not consider a situation in which a user manual incidentally distributed with an expensive product could be considered publicly accessible or what effect a confidentiality provision in the manual would have on its public accessibility. *Id.* Indeed, there is no record evidence or argument that the confidentiality provision would make it more likely that an interested person could access Sourcefire exercising reasonable diligence.

Accordingly, the controlling question remains, was Sourcefire “disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it”? *Acceleration Bay*, 908 F.3d at 772. The answer is no. Sourcefire was only obtainable by purchasing the Sourcefire 3D appliance, and there is no record evidence demonstrating that “reasonable diligence” could extend so far as to encompass paying over \$25,000, particularly for a reference that was disparaged as only being of interest to those “operating the suite as a whole” (*i.e.* customers who

purchased the Sourcefire product). Appx4701 (“There are two manuals, one is an installation guide and the other is an administrator manual. But the documentation is very long, more than 900 pages, and is geared to operating the suite as a whole. If the manual is needed to answer specific configuration issues or questions, the search for information can be very time-consuming.”).

For at least the foregoing reasons, Sourcefire was not publicly accessible and is not a printed publication. The Board’s decisions finding the ’552 and ’713 Patents obvious over Sourcefire should, therefore, be reversed.

B. Sourcefire Does Not Render the Challenged Claims Obvious

Each independent claim of the ’513 and ’772 Patents requires a determination that a packet includes a specified TLS version value. Sourcefire never makes any such determination. The Board’s decision nevertheless finding this element obvious is unsupported by substantial evidence, and suffers from fatal factual, technical, and legal errors that require reversal of the Final Written Decisions.

1. Sourcefire Does Not Determine Whether a Packet Includes a Specified TLS-Version Value

The Board factually and materially erred at the very outset of its analysis, citing the Oral Hearing Transcript as allegedly establishing that “[i]t is undisputed that such reassembled or reconstructed messages consist of packets.” Appx47 (citing Appx803 at 35:4–6 and Appx807 at 39:14–16); *see also* Appx89. This

fundamental premise is simply not true because while reassembled messages are assembled from information within packets, after the packets are reassembled “there’s no conception of a packet. It is a message.” Appx840 at 72:14–23; *see also* Appx841–842 at 73:17–74:8. Sourcefire itself drives home this very point:

The stream preprocessor collects and reassembles all the packets that are part of a TCP session’s server-to-client communication stream, client-to-server communication stream, or both. ***This allows the rules engine to inspect the stream as a single, reassembled entity rather than inspecting only the individual packets*** that are part of a given stream.

Appx461 (quoting Appx2064-2065).

Based on this incorrect understanding of the difference between packets and a reassembled messages, the Board made its second fatal factual error, namely that “Sourcefire teaches determining that the reassembled handshake message comprises TLS version data *by extracting that data from the first packet of the message.*” Appx48. It does not, and the record evidence only supports the opposite conclusion. Appx461 (quoting Appx2064-2065). Indeed, the portion of the Hearing Transcript cited in support demonstrates exactly the opposite of what the Board cited it for:

JUDGE LEE: I mean, it seems to me what you’re saying is Sourcefire’s not the same thing because Centripetal’s invention extracts TLS version data from the first packet in the message and it’s called a packet and in Sourcefire you’re extracting TLS version information from the header that’s in the first packet of a message but when you’re doing that, it’s a message and not a packet. **So, you’re extracting it from the message not a packet.**

MR. PRICE: **That’s correct, and because you’re extracting it from a fully reconstituted message, you never make a determination of what is in any one of the packets that’s being looked at by the rule....** So, for the Sourcefire method, you receive a packet, you apply one of these rules, you don’t know if the packet that you’re actually apply to that rule to has the information that you’re looking for. Because what you’re doing is, you’re going back to the data that was extracted from a reconstituted message which at that time you don’t have any concept of the packets anymore.

Appx808 at 40:3–20 (emphasis added); *see also* Appx809-810 at 41:20–42:9.

It is undisputed that Sourcefire teaches reassembling received packets to perform its security analysis. Appx42 (citing Appx6606-6607 at 120:19–123:17). When Sourcefire performs its analysis, Sourcefire only returns information that was extracted from a reassembled message associated with the communications session, not information from a particular packet. Appx481 (citing Appx2025, Appx6724-6725 at ¶ 115).

Throughout and following this process, Sourcefire never determines whether any particular packet includes the returned TLS-version value. Appx2064-2065; *see also* Appx6606-6607 at 120:19-123:17 (confirming that Sourcefire’s SSL preprocessor “has to do [with] TCP reconstruction” and does so using “the TCP stream processor”). And because not every packet in the session will include the TLS-version value being used to encrypt a particular session, Sourcefire’s technique fails to determine whether **any** packet includes the specified value. For at least this reason, even in the case “that a handshake message could fit into a

single application packet” (see Appx46), Sourcefire never makes a determination that the single application packet includes a specified TLS-version value because Sourcefire has no concept of individual packet inspection.

And as discussed directly below, whether or not a user of the Sourcefire system could deduce in some undisclosed *post hoc* analysis that “such a packet would include a TLS version value” there is no record evidence even arguing, let alone demonstrating by a preponderance of the evidence, that a POSA would have modified Sourcefire’s express teachings to make such a determination.

2. Petitioner Did Not Demonstrate Any Motivation to Modify Sourcefire, But Instead Used Hindsight to Fill-In Missing Elements.

The Board erred as a matter of law by misstating the test for obviousness. In particular, the Board asserted that whether or not Sourcefire recognizes or deduces that the “relevant data is located in the first packet of the message... is irrelevant” and that “the relevant question is whether a *person of ordinary skill* would have been taught the recited determination (i.e., determining that a packet comprises TLS version data) based on Sourcefire and his/her own knowledge.” Appx48 (citing *Keller*, 642 F.2d at 425). The Board is wrong.

The relevant question, given that Sourcefire does not teach the claimed “determination,” is whether or not a POSA would have been motivated to **modify** Sourcefire’s disclosed technique to reach the challenged claims. See *Game & Tech.*,

926 F.3d at 1381 (“[A] patent can be obvious in light of a single prior art reference if it would have been obvious to modify that reference to arrive at the patented invention.”). But Petitioner made no allegation whatsoever that a POSA would have modified Sourcefire to additionally make a determination that any particular packet includes a specified TLS-value, and the Board has cited no evidence that a POSA would have modified Sourcefire to make such a determination.

Simply put Sourcefire **never** determines whether individual packets in a communication include a specific TLS version value, which is explicitly recited in each of the challenged claims for the ‘552 and ‘713 Patents. Nor is there any evidence in the record that a POSA reading Sourcefire could or would have **modified** its technique in order to reach the challenged claims. Indeed, because Sourcefire’s technique works in its own way—by reconstructing all of the packets in a communication—there is no reason, let alone motivation, to modify Sourcefire to in order to determine whether any particular packet includes a specified TLS-version value. The challenged claims are not obvious.

Indeed, the Board’s conclusion, that the claims are obvious because a POSA would have been known where to look for the data in a packet, expressly violates this Court’s decision in *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016). In *Arendi*, this Court held that “common sense” may not be used to “supply a limitation that was admittedly *missing* from the prior art” where the

limitation “‘plays a major role in the subject matter claimed’ and ‘affects much more than’” the limitation itself. *Id.* at 1362. The “determining” limitation fits this definition because it is not only missing from Sourcefire, it “plays a major role in the subject matter claimed” because further claimed actions depend on making the claimed determination (*i.e.* applying a “packet-transformation function” responsive to the determination). *See, e.g.*, Appx145-147 at Claims 1, 8, and 15; Appx159-160 at Claims 1, 8, and 15. Accordingly, whether or not a POSA “would have been taught the recited determination (*i.e.*, determining that a packet comprises TLS version data) based on Sourcefire and his/her own knowledge” is inadequate as a matter of law to demonstrate that “it would have been obvious to modify [Sourcefire] to arrive at the patented invention.” *Compare Appx48 with Arendi*, 832 F.3d at 1361.

Further demonstrating the fact that the “determination” step “plays a major role in the subject matter claimed” is that it reflects the fundamental difference between packet filters that “operate on individual IP packets,” which “do not degrade network performance as much as stateful IPS systems” such as Sourcefire. Appx442; *see also id.* at Appx442-446; Appx3667–3669 at 2:27–63, 3:4–4:35, 5:27–29, 6:9–33. There can be no dispute that the challenged claims involve operations on individual packets while Sourcefire is an IPS, which requires TCP packet reassembly so that “[t]he entire stream of data is analyzed.” *Compare*

Appx145 at Claim 1 (reciting the application of an operator to packets) and Appx159 at Claim 1 (reciting a determination that “the first packet comprises data corresponding to a... (TLS)-version value) *with* Appx2064-2065 (disclosing that Sourcefire “inspect[s] the stream as a single reassembled entity rather than inspecting only the individual packets that are part of a given stream”) *and* Appx6607 at 121:21–123:17 (admitting that Sourcefire is a stateful IPS **has to** inspect application layer traffic with TCP reconstruction).

The Board also erred by improperly ignoring objective indicia of non-obviousness with a direct nexus to this claim element. In particular, the Board repeated Centripetal’s argument that “the salutary benefits of Centripetal’s [praised product] are made possible in large part by the ’552 Patent’s network layer, packet-by-packet, rule enforcement that foregoes deep inspection at the application layer” and summarily dismissed it as allegedly being conclusory for failing to disclose the underlying facts and data upon which it was based. Appx60. To the contrary, however, Centripetal’s argument was supported by its expert, Dr. Orso, who in turn relied on unrebutted underlying evidence to support his unrebutted opinions. *See* Appx6727–6734 at ¶¶126–133 (citing Appx6900–6908, Appx6909–6918, Appx7070–7092 and the ’552 and ’713 Patents).

Dr. Orso first explained that there was long-felt need for a scalable technique for providing proactive network protection. Appx6729–6730 at ¶¶126–127 (citing

Appx7074–7075; Appx6902). Then he explained that the long-felt need was solved by the packet filtering technique disclosed in the patents and “there is no need for time- and resource-intensive packet reassembly procedures, such as those used in Sourcefire.” Appx6732; *see also* Appx442 (explaining that “[o]ne major benefit of stateless packet-filtering firewalls is that they do not degrade network performance as much as stateful IPS systems” (citing Appx3667 at 2:54-55)).

Next, Dr. Orso cited Exhibits 2006 and 2007, each of which supports his opinion that the application of the claimed rules to individual packets differentiates Centripetal’s RuleGATE from traditional IPS security devices like Sourcefire, which perform “deeper inspection of the application layer.” Appx6733; Appx6913-6914; *see also* Appx6906 (“Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren’t designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal Networks’ Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules.”).

Finally, the Board inexplicably declined to consider the skepticism of Petitioner’s expert, who admitted he believed that the technique of the challenged claims “couldn’t possibly work”:

Q. So my question is, where does the '552 patent sit in -- on this divide between a packet filter that doesn't keep state information and a stateful inspection firewall, or does it not sit at all on the same plane?

A. The question never crossed my mind at the time I wrote the declaration because, of course, in 2012, system **couldn't possibly work** in a stateless manner. And, in particular, you know, much of the functionality described in the patent couldn't possibly work unless some state was being kept.

Appx6604 at 109:21-110:13 (emphasis added).

The Board's stated reason for ignoring this skepticism was that it did not consider Dr. Staniford's testimony as expressing "skepticism regarding the viability of Centripetal's products, which practice the "'552 [p]atent," nor did he "opine that [Centripetal's] solution was impossible," stating that "Dr. Staniford's testimony concerned Sourcefire." Appx61. But the passage reproduced above **explicitly** concerns the concrete implementation of the '552 Patent's claims, not the teachings or operation of Sourcefire. Only later did Dr. Stanford state that he couldn't "say whether it's absolutely impossible to run Sourcefire in a stateless mode" but that "no POSA worth a damn would propose to do that because it's not a useful way to detect attacks anytime recently." Appx6607 at 123:10-17. Thus, not only did Dr. Staniford express skepticism about the approach to network security recited in the challenged claims, he said that it "couldn't possibly work" and that "no POSA worth a damn" would have operated Sourcefire as claimed in the '552 and '713 Patents. Appx6604 at 109:21-110:13; Appx6607 at 123:10-17.

Finally, the Board’s citation to *Fox Factory* is inapposite because Centripetal did not rely on, and did not need to rely on, any **presumption** of a nexus. Appx61. Instead, Centripetal proved the nexus “by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention.’” *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373–74 (Fed. Cir. 2019). In particular, Centripetal demonstrated, via un rebutted evidence and expert testimony, that “the best-in-class performance of Centripetal’s TIG owes in large part to the fact that the ’552 Patent’s packet-filtering rules are applied on a packet-by-packet basis, allowing the TIG to operate as a ‘network filter’ rather than a traditional IPS, such as Sourcefire, that performs ‘deeper inspection of the application layer.’” Appx494–495 (citing Appx6732–6733 at ¶ 130 and Appx6914). Only by ignoring the foregoing testimony and evidence could the board conclude that Dr. Orso’s testimony was conclusory and lacked explanation. Appx60. To the contrary, Centripetal established a “legally and factually sufficient connection between the evidence and the patented invention.” *Fox Factory*, 944 F.3d at 1373 (internal quotations omitted).

Given the foregoing, the Board’s decision finding all claims of the ’552 and ’713 Patents must be reversed. The undisputed record evidence demonstrates that Sourcefire extracts information from reassembled messages and never makes a determination that any packet includes a specified TLS-version value. Nor is there

any evidence in the record, let alone substantial evidence, supporting a finding that it would have been obvious to modify Sourcefire to make the claimed “determination.” Objective indicia of non-obviousness, including evidence of long-felt need, industry praise, and skepticism of Petitioner’s expert only clarify the distinctions between Sourcefire, which performs “deeper inspection of the application layer,” and the packet filtering techniques of ’552 and ’713 Patents, which helped enable “the highest performance network filter that ESG has tested or seen in action to date.” Appx6907.

C. Sourcefire Does Not Disclose the Claimed Operator

Substantial evidence does not support the Board’s conclusion that Sourcefire teaches an “operator” that specifies (1) one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values as well as (2) at least one packet-transformation function. *See* Appx145-147 at Claims. Examples of this type of operator are reproduced below:

HTTP-EXFIL Operator	REQUIRE-TLS-1.1-1.2 Operator
<pre>Operator HTTP-EXFIL(ip-packet): Inspect app-pkt(ip-packet) match GET return ALLOW; Inspect app-pkt(ip-packet) match POST return BLOCK; Inspect app-pkt(ip-packet) match PUT return BLOCK; Inspect app-pkt(ip-packet) match DELETE return BLOCK; Inspect app-pkt(ip-packet) match CONNECT return BLOCK; Return BLOCK; End Operator HTTP-EXFIL;</pre>	<pre>Operator REQUIRE-TLS-1.1-1.2(ip-packet): Inspect app-pkt(ip-packet) match 1.0 return BLOCK; Inspect app-pkt(ip-packet) match 1.1 return ALLOW; Inspect app-pkt(ip-packet) match 1.2 return ALLOW; Return BLOCK; End Operator REQUIRE-TLS-1.1-1.2;</pre>

Appx453 (citing Appx143 at 7:31–38 and 7:64–8:6). One important consequence of using an “operator” to specify the TLS-version value and the corresponding

packet-transformation function is that rules can apply different packet transformation functions for different TLS-version values. Appx472–473 (citing Appx143 at 7:31–38 and 7:64–8:6 and Appx6717–6718 at ¶ 105).

Sourcefire does not, and cannot, disclose the recited “operator” that specifies a “packet transformation function.” Sourcefire works on the basis of Snort rules that include a “Rule Header” and “Rule Options”:

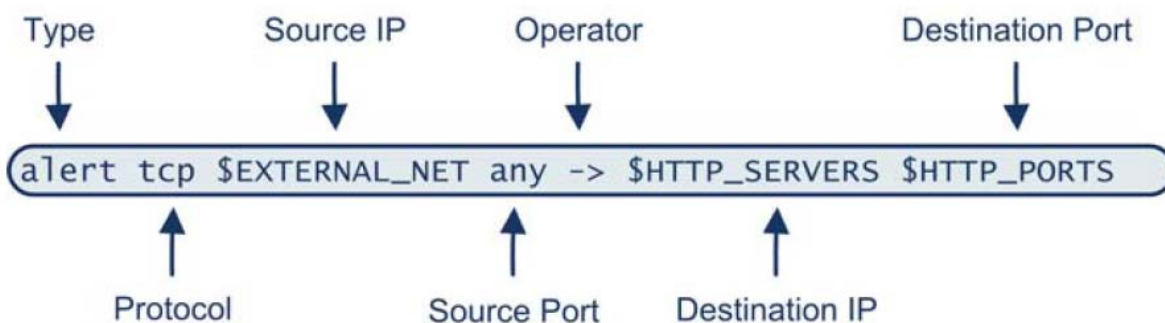
Rule Header

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
```

Rule Keywords and Arguments

```
(msg:"WEB-IIS newdsn.exe access";  
flow:to_server,established; uricontent:"/scripts/  
tools/newdsn.exe"; nocase; metadata:service http;  
reference:bugtraq,1818; reference:cve,1999-0191;  
reference:nessus,10360; classtype:web-application-  
activity; sid:1024; rev:10; )
```

Appx472 (citing Appx2189-2190). One of the fields in the Rule Header is the Rule Type, or Action:



Appx2191. The Rule Action is the action that is taken “if the packet data matches **all** the conditions specified in a rule”:

An *intrusion rule* is a specified set of keywords and arguments on a 3D Sensor with the IPS component that detects attempts to exploit vulnerabilities on your network by analyzing network traffic to check if it matches the criteria in the rule. IPS compares packets against the conditions specified in each rule and, **if the packet data matches all the conditions specified in a rule**, the rule triggers. If a rule is an *alert rule*, it generates an intrusion event. If it is a *pass rule*, it ignores the traffic.

Appx2188 (bold emphasis added). In other words, because Sourcefire only supports one rule action per rule, it is apparent that it does not disclose the claimed operator which specifies the TLS version value and the packet transformation function. *Id.* The Board’s conclusory acceptance of Petitioner’s attorney argument to the contrary is unsupported by any evidence, let alone substantial evidence. See Appx51 (citing Appx570).

The substantial evidence standard “requires that the grounds upon which the [PTAB] acted be clearly disclosed and adequately sustained.” *In re NuVasive, Inc.*, 842 F.3d 1376, 1382 (Fed. Cir. 2016). The Board’s bare citation to ten pages of Sourcefire does not meet this standard because it does not point to, let alone explain, where in those ten pages the relevant disclosure exists. See Appx50-51 (citing Appx2188–2197). That is, the Board’s acceptance, without analysis, of Petitioner’s **attorney argument** that Sourcefire “can use the same rule to specify different packet transformation functions for different application-layer-packet-

header criteria” violates the APA because the “PTAB’s adoption” of Petitioner’s attorney argument does not “transform [that] argument into factual findings or supply the requisite explanation that must accompany such findings.” *See Icon Health & Fitness, Inc. v. Strava, Inc.*, 849 F.3d 1034, 1043 (Fed. Cir. 2017).

To the contrary, the evidence cited in Centripetal’s Sur-Reply and reproduced above directly contradicts the Board’s finding that Sourcefire “can use the same rule to specify different packet transformation functions for different application-layer-packet-header criteria.” *Compare* Appx606 (citing Appx2188 and Appx2190) *with* Appx51. The Board’s decision to ignore this evidence while crediting Petitioner’s attorney argument that purports to characterize a broad swath of Sourcefire violates the APA and does not, therefore meet the substantial evidence standard. Because substantial evidence does not support the Board’s determination that the challenged claims of the ’552 Patent are obvious over Sourcefire, the Board’s rejection of Claims 1–21 of the ’552 Patent must be reversed.

VI. CONCLUSION

For the foregoing reasons, Centripetal respectfully requests that this Court reverse the Board’s decision finding claims 1–21 of the ’552 Patent and 1–20 of the ’713 Patent obvious over Sourcefire or at least vacate the decision and remand to the Board for further consideration.

Respectfully submitted,

Dated: July 10, 2020

/s/ James Hannah

Paul J. Andre

James Hannah

Kramer Levin Naftalis & Frankel LLP

990 Marsh Road

Menlo Park, California 94025

Tel: (650) 752-1700

Fax: (650) 752-1800

pandre@kramerlevin.com

jhannah@kramerlevin.com

Jeffrey H. Price

Kramer Levin Naftalis & Frankel LLP

1177 Avenue of the Americas

New York, NY 10036

Tel: 212.715.7502

Fax: 212.715.8302

jprice@kramerlevin.com

Attorneys for Appellant

Centripetal Networks, Inc.