NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

CENTRIPETAL NETWORKS, INC.,
Appellant

v.

CISCO SYSTEMS, INC.,
Appellee

2020-1635, 2020-1636

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

Decided: March 10, 2021

JAMES R. HANNAH, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, for appellant. Also represented by PAUL J. ANDRE; JEFFREY PRICE, New York, NY.

PATRICK D. MCPHERSON, Duane Morris LLP, Washington, DC, for appellee. Also represented by CHRISTOPHER JOSEPH TYSON; MATTHEW CHRISTOPHER GAUDET, Atlanta, GA; JOSEPH POWERS, Philadelphia, PA.

Before MOORE, SCHALL, and TARANTO, *Circuit Judges*.

TARANTO, *Circuit Judge*.

Centripetal Networks, Inc. owns U.S. Patent Nos. 9,124,552 and 9,160,713, which address cybersecurity techniques for filtering encrypted packets passing between a secured and an unsecured network. In July 2018, Cisco Systems, Inc. filed petitions for inter partes reviews of the '552 and '713 patents. For all claims of both patents, Cisco asserted unpatentability under 35 U.S.C. § 103 for obviousness based on a user manual for an earlier security system—a manual that Cisco asserted was a prior-art "printed publication." 35 U.S.C. § 311(b). The Patent Trial and Appeal Board instituted both requested inter partes reviews and, in its final written decisions, agreed with Cisco about the printed-publication status of the user manual and about unpatentability of all claims. *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01436, 2020 WL 402817 (P.T.A.B. Jan. 23, 2020) (*'552 Decision*); *Cisco Systems, Inc. v. Centripetal Networks, Inc.*, IPR2018-01437, 2020 WL 402317 (P.T.A.B. Jan. 23, 2020) (*'713 Decision*). We affirm.

I

A

The patents address aspects of the now-common process of sending messages across networks, specifically across the Internet, using protocols that split up a message's content into packets for transmission. J.A. 6682 ¶ 47; J.A. 6823. When packets arrive at their destination, they are assembled to recreate the original message. *See* J.A. 2064. Two common preexisting protocols, which allow encryption of the transmitted data, are relevant here: Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS). *See* '552 patent, col. 7, lines 53–60.

Because the '713 patent issued from a continuation of the application that issued as the '552 patent, the patents

share a specification, and when citing that specification, we will generally cite only the '552 patent. The patents are concerned with "filtering network data transfers" and the passage of information between a secured network (*e.g.*, a private company's network) and an unsecured network (*e.g.*, the larger Internet). '552 patent, Abstract; '713 patent, Abstract; *see also* '552 patent, col. 1, lines 62–64. The specification focuses, in particular, on preventing a type of cyberattack known as an "exfiltration," which involves stealing information (extracting it without authorization) as it exits a secure network, using "popular network data transfer protocols" to disguise the theft "as normal network behavior." *Id.*, col. 1, lines 15–23. Previous cybersecurity systems, the patents say, inadequately protected against such attacks because they tended to interpret the exfiltration as ordinary network behavior and did not account for vulnerabilities in the conventional version of TLS, *i.e.*, TLS version 1.0. *Id.*, col. 1, lines 23–25; *id.*, col. 6, lines 40–47.

The patents describe a solution in which packets entering or exiting a secure network are first received at a packet secure gateway, which may include "one or more computing devices configured to receive packets." *Id.*, col. 3, lines 42–44. The gateway also receives a "dynamic security policy" from a "security policy management server," *id.*, col. 4, lines 53–55, which provides the "packet filter" in the gateway with "one or more rules" to determine where (to which "operators") packets "having specified information" should be sent, *id.*, col. 5, lines 6–16. The specified information gathered from a packet may include a "five-tuple," which may comprise "one or more values selected from": the protocol type of the packet, the Internet Protocol (IP) address of the source of the packet, "one or more source port values," the IP address(es) of the destination(s) of the packet, and "one or more destination ports." *Id.*, col. 5, lines 34–42. Based on the information collected from the packet, the gateway system "determines" which operator to direct the packet to, *id.*, col. 5, lines 9–16, and the operator

then applies one or more filtering rules to the packet to "allow" or "block" the packet, *see*, *e.g.*, *id.* col. 5, lines 62–67; *id.* col. 6, lines 11–16. For example, a rule may require that a packet use "version 1.1 or 1.2 of the Transport Layer Security (TLS) protocol" in order to be allowed to continue, because "the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions." *Id.*, col. 6, lines 27–47.

Independent claim 1 of the '552 patent recites:

> 1. A method, comprising:
>
> at a computing device comprising at least one processor, a memory, and a communication interface:
>
> receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets;
>
> responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory, applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations;
>
> and
>
> 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, applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.

Id., col. 11, lines 5–35. Claims 8 and 15 are the only other independent claims in the '552 patent. Claim 8 claims an "apparatus" that performs the claim 1 method and claim 15 claims "non-transitory computer-readable media" containing instructions that, when executed, perform the claim 1 method. *Id.*, col. 12, line 54 through col. 13, line 15; *id.* col. 13, lines 39–67. No additional limitations in the dependent claims of the '552 patent are relevant to Centripetal's appeal.

Claim 1 of the '713 patent recites:

> 1. A method comprising:
>
> receiving, by a computing system provisioned with a plurality of packet-filtering rules, a first packet and a second packet;
>
> responsive to a determination by the computing system that the first packet comprises data corresponding to a transport layer security (TLS)-version value for which one or more packet-filtering rules of the plurality of packet-filtering rules indicate packets should be forwarded toward their respective destinations, forwarding, by the computing system, the first packet toward its destination; and

> responsive to a determination by the computing system that the second packet comprises data corresponding to a TLS-version value for which the one or more packet-filtering rules indicate packets should be blocked from continuing toward their respective destinations, dropping, by the computer system, the second packet.

'713 patent, col. 11, lines 8–25. Independent claims 8 and 15 of the '713 patent are substantially similar to claim 1; for present purposes, they are system and non-transitory computer-readable media forms of method claim 1. *See id.*, col. 12, lines 29–47; *id.*, col. 13, lines 44–61.

B

In July 2018, Cisco filed petitions for inter partes reviews of all claims (claims 1–21) of the '552 patent and all claims (claims 1–20) of the '713 patent. Cisco argued that the claimed inventions of all claims would have been obvious to a relevant artisan in view of the User Guide for the Sourcefire 3D System—a manual referred to in the matters before us as "Sourcefire."

Sourcefire describes a system that monitors network activity with packet-filtering devices called "3D-Sensors" that record network activity and identify (and call attention to) "intrusion events" based on an "intrusion policy applied to a detection engine on the sensor that is monitoring a specific network segment." J.A. 1460, 1683. In this system, packets traveling through the network pass through three layers that decode them, J.A. 1683, 1685, then pass through preprocessors that "normalize traffic at the application layer and detect protocol anomalies," J.A. 1685, and finally arrive at a "rules engine" that "inspects the packet headers" and "determine[s] whether they trigger any of the shared object rules or standard text rules," J.A. 1685–86. At any of these steps, a packet could cause the system "to generate an event, which is an indication that the packet or its contents" may be a security risk. J.A. 1687.

When packets arrive at Sourcefire's rules engine, the engine determines whether values in the packet header trigger one or more "intrusion rules." J.A. 1686, 1940, 2188. Intrusion rules may have two parts: (1) the rule header, which includes the five-tuple values (protocol, source and destination IP addresses, source and destination ports), the rule's action (*e.g.*, drop, alert and allow, ignore and allow), and direction indicators; and (2) the rule options part, which contains, *e.g.*, keywords and their arguments and event messages. J.A. 2189; *see also* J.A. 2188–96. Keywords in intrusion rules can be used by the preprocessor (called the Secure Sockets Layer (SSL) preprocessor) and by the rules engine to filter packets according to their encryption protocol version (for example, their TLS version). J.A. 2252. Sourcefire permits users to write their own custom intrusion rules, J.A. 2188–96, so a user could use a keyword like "ssl_version" in an intrusion rule to cause the SSL preprocessor to match the protocol version information contained in the application headers of the packets against the protocol of the assembled packets for an encrypted session (a reassembled stream of messages known as a handshake), J.A. 2254–55; *see also* J.A. 1918, 2024–28, 2127.

In its petitions for inter partes reviews, Cisco argued that the claims of the '552 and '713 patents recite subject matter that would have been obvious in view of Sourcefire because Sourcefire describes a cybersecurity system that can be configured to meet every limitation in the claims. *'552 Decision*, 2020 WL 402817, at *8; *'713 Decision*, 2020 WL 402317, at *6–7. Specifically, Cisco relied on Sourcefire as disclosing, to a relevant artisan, the idea of writing custom intrusion rules that would permit the Sourcefire system to determine the TLS-version values of the packets it received based on keywords and to use the rules engine as an operator to apply packet-filtering rules based on those determinations. *'552 Decision*, 2020 WL

402817, at *15–16; *'713 Decision*, 2020 WL 402317, at *6–7.

After the Board instituted the requested inter partes reviews, Centripetal argued that Sourcefire was not a "printed publication" at the priority date for the patents at issue, *see* 35 U.S.C. § 102(a)(1); 35 U.S.C. § 102(b) (2006), as required for non-patent prior art in IPRs under 35 U.S.C. § 311(b). J.A. 434–38; *see also '713 Decision*, 2020 WL 402317, at *3.[1] Centripetal contended that Sourcefire (the document) was costly and was distributed only to those who bought certain products from Sourcefire (the company) and, therefore, the document was not publicly accessible because a relevant artisan could not have obtained it with reasonable diligence. J.A. 434–38.

In IPR-1436 (addressing the '552 patent), Centripetal did not dispute that Sourcefire teaches a processor, memory, and communication interface; nor did it dispute that Sourcefire teaches "receiving, via the communication interface a plurality of [HTTPS] packets." *'552 Decision*, 2020 WL 402817, at *14–15. Centripetal argued, however, that Sourcefire does not teach the "determination" limitations of the claims, specifically the requirements of (1) a "determination" that a plurality of HTTPS packets "have packet-header-field values corresponding to a packet-filtering rule" and (2) a "determination" that some of those packets "have one or more application-header-field values corresponding to one or more TLS-version values." *See* J.A. 456, 458. According to Centripetal, Sourcefire teaches

---

[1] The version of 35 U.S.C. § 102 pre-dating the amendments made in 2011 (effective March 16, 2013) applies in both of these matters, given that the application that issued as the '552 patent was filed March 12, 2013, and the '713 patent is the child of the '552 patent. *See '552 Decision*, 2020 WL 402817, at *4 n.1. The current version of § 102 continues to use the phrase "printed publication."

extracting version information from a reassembled stream of packets ("handshake and key exchange messages," J.A. 2025), whereas the claims require a determination of version information to be made for individual packets. J.A. 461–62.

Centripetal alleged an additional deficiency in Sourcefire's teaching of the claim limitations. It contended that Sourcefire does not teach the claimed "operator," because the claims require that the operator specify both "application-header-field-value criteria" and "a packet transformation function," and the Sourcefire system is "not capable of designing a packet-filtering rule specifying an operator that applies different packet transformation functions based on different application-layer-packet-header criteria." J.A. 471–73. Centripetal further argued that Cisco had not shown that a relevant artisan would have been motivated to modify the teachings of Sourcefire to arrive at the claims. J.A. 481. And Centripetal advanced what it urged were objective indicia of nonobviousness, including praise for its product addressing TLS vulnerabilities. J.A. 494–95.

In IPR-1437 (addressing the '713 patent), Centripetal made similar arguments. *See* J.A. 7394–99, 7403–06.

C

In IPR-1436, the Board first determined that Cisco had met its burden to show that Sourcefire was a printed publication. *'552 Decision*, 2020 WL 402817, at *8–12. Specifically, the Board found that Sourcefire, a user guide, was publicly accessible in that it was available to purchasers of Sourcefire 3D Systems and was, in fact, distributed on CD-ROM to 586 system purchasers between April 2011 and March 2013, *id.* at *9–10; no confidentiality restrictions prevented purchasers from reproducing and distributing the document "for non-commercial use," *id.* at *10 (citing J.A. 1429); and Sourcefire advertised its products and their accompaniment by extensive documentation, *id.* at *11;

J.A. 4695–99. The Board rejected Centripetal's argument that the cost of obtaining Sourcefire (the document) was prohibitive; the Board found that it could be acquired by purchasing products that cost between $1,385 and £25,000, that 586 customers actually acquired it, and that Centripetal had not shown that an interested relevant artisan was not reasonably able to obtain the material. *Id.* at *12 & n.9.

After determining that Sourcefire qualified as prior art, the Board addressed the disputed limitations in claim 1 (and claims 8 and 15). *Id.* at *14–22. Regarding the determination limitations, the Board explained that nothing in the claims requires that each individual packet be inspected or that TLS (or SSL) version information be extracted from application-header-values of individual packets, rather than a reassembled stream (handshake message). *Id.* at *17. Reassembled streams of messages, the Board continued, themselves consist of individual packets, and a relevant artisan would have known that the TLS-version information is always contained in the packet header of the first packet in the message, as Centripetal acknowledged. *Id.* at *18. Accordingly, the Board found that a relevant artisan would have understood Sourcefire, even in describing the extraction of version information from the reassembled message, as teaching the claim requirement of extraction from the first packet. *Id.* at *18–19.

Regarding the claimed "operator," the Board adopted Centripetal's claim construction, construing the term to refer to "a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria." *Id.* at *5–6. Applying that construction, the Board found that Sourcefire's keyword and argument functions (in particular, ssl_version keywords) permitted the system to (1) indicate application-header-field-value criteria (*e.g.*, the version of TLS)

and (2) apply a "packet transformation function," *e.g.*, blocking the packets, as specified by the claims. *Id.* at *19. The Board also rejected Centripetal's argument that Sourcefire could not teach an operator because the "rule action" was specified in the "rule header," so that Sourcefire could apply only "one rule action" per rule (*e.g.*, could only allow certain packets, rather than allow and block some). *Id.* at *20. The Board found that Centripetal had presented no evidence to support this argument and that Cisco had shown support in Sourcefire for using different ssl_version keywords to "allow," "pass," or "drop" packets. *Id.*

Finally, the Board found that Cisco had met its burden to show that a relevant artisan would have been motivated to modify Sourcefire to meet the '552 patent's claim limitations. *Id.* at *21–22. Citing the declaration from Cisco's expert (Dr. Staniford), the Board found that the known vulnerabilities of early versions of protocols like TLS, along with the ordinary creativity of a relevant artisan, would be sufficient to motivate that artisan to use Sourcefire to write rules blocking packets with a vulnerability like that of TLS 1.0. *Id.* The Board also found that Centripetal's objective indicia of nonobviousness—particularly the praise for its RuleGATE product—were not entitled to much weight, noting the lack of a persuasive basis for finding the nexus of cited objective indicia to the claims of the '552 patent. *Id.* at *22–24. The Board then addressed the additional limitations in the remaining dependent claims and found obviousness as to those claims as well. *Id.* at *24–26.

In IPR-1437, the Board's finding and reasoning were similar to those in IPR-1436. *See '713 Decision*, 2020 WL 402317, at *3–13.

The Board issued its final written decisions as to both IPR-1436 and IPR-1437 on January 23, 2020. Centripetal timely appealed both decisions. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A) and 35 U.S.C. §§ 141(c), 319.

II

We review the Board's final written decisions under the Administrative Procedure Act, "hold[ing] unlawful and set[ting] aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law . . . [or] unsupported by substantial evidence." 5 U.S.C. § 706; *Dickinson v. Zurko*, 527 U.S. 150, 164–65 (1999). We review the Board's legal conclusions de novo and factual findings for substantial evidence. *Nobel Biocare Services AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1374 (Fed. Cir. 2018). Whether a reference qualifies as a "printed publication" is a legal conclusion based on factual findings. *Jazz Pharms., Inc. v. Amneal Pharms., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018). "The underlying factual findings [in a printed-publication analysis] include whether a reference was publicly accessible." *Nobel*, 903 F.3d at 1375. Similarly, the ultimate determination of whether a claimed invention would have been obvious is a legal one reviewed de novo, but underlying factual determinations are reviewed for substantial-evidence support. *PersonalWeb Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1381 (Fed. Cir. 2019).

On appeal, Centripetal argues that: (1) the Board erred by concluding that Sourcefire is a printed publication, *see* Centripetal Opening Br. 15–21; (2) Sourcefire does not teach a "determination" that a packet includes a specified TLS-version value, *id.* at 21–24; (3) Cisco did not show a motivation to modify Sourcefire and the Board overlooked important objective indicia of nonobviousness, *id.* at 24–31; and (4) Sourcefire does not disclose the operator described in the '552 patent, *id.* at 31–34.[2] We reject these challenges.

---

[2] In making their respective arguments on appeal, the parties do not distinguish between the Board's

A

Centripetal first contends that Sourcefire was not a printed publication because it was available only to those willing to pay $25,000 for the accompanying product and was kept password-protected on Sourcefire's website, preventing access to the relevant public. Centripetal Opening Br. 15–16. We reject this argument.

Whether a reference is a printed publication "involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public." *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). "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." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (cleaned up). For a reference to be publicly accessible, it must be "'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) (quoting *Jazz Pharms.*, 895 F.3d at 1355–56); *see also Kyocera Wireless Corp. v. Int'l Trade Comm'n*, 545 F.3d 1340, 1350 (Fed. Cir. 2008). A reference need not be catalogued or indexed to be a printed publication; "a printed publication need not be easily searchable after publication if it was sufficiently disseminated at the time of its publication." *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1365 (Fed. Cir. 2014); *see also In re Lister*, 583 F.3d 1307, 1312 (Fed. Cir. 2009); *Klopfenstein*, 380 F.3d at 1348. Limited distributions of a reference may suffice. *Samsung Elecs. Co. v.*

---

decisions in IPR-1436 and IPR-1437, except where relevant. Centripetal Opening Br. 3; Cisco Response Br. 6 n.1. We consider the decisions together unless otherwise noted.

Infobridge Pte. Ltd., 929 F.3d 1363, 1374 (Fed. Cir. 2019). In determining whether interested persons could have accessed the publication, we consider factors such as the expertise of the target audience, the avenues of distribution (*e.g.*, at a trade show), the duration of dissemination, and expectations of confidentiality or restrictions on recipients' sharing of the information. *GoPro, Inc. v. Contour IP Holding LLC*, 908 F.3d 690, 694–95 (Fed. Cir. 2018).[3]

---

[3] *See*, *e.g.*, *GoPro*, 908 F.3d at 694–95 (catalog distributed at a trade show that was only open to "dealers" of action sports vehicles and related accessories was a printed publication because there were no restrictions on the catalog's distribution, there were over 1,000 attendees, and there was no evidence that one interested in the art of digital cameras could not have obtained the catalog with reasonable diligence); *Jazz Pharms.*, 895 F.3d at 1357–59 (Affordable Care Act materials available on the FDA's website and published via constructive notice in the Federal Register were printed publications because the materials were "widely disseminated to persons of ordinary skill for a substantial time with no reasonable expectation of confidentiality"); *Klopfenstein*, 380 F.3d at 1350 (slideshow displayed at a conference for three days was a printed publication because the slide was displayed for a matter of days, the attendees included interested persons of skill in the art, there was no reasonable expectation that the slide would not be copied, and the slide could be copied with relative simplicity); *Massachusetts Inst. of Tech. v. AB Fortia (MIT)*, 774 F.2d 1104, 1108–09 (Fed. Cir. 1985) (paper orally presented at a conference and distributed to only six persons who requested the paper was a printed publication, because "between 50 and 500 persons interested and of ordinary skill in the subject matter were told of the existence of the paper . . . and the document itself was

Here, the Board found, based on testimony from a Sourcefire company employee, that each of the 586 customers who purchased a range of Sourcefire products over a relevant two-year period received a CD-ROM containing the user guide, which explicitly stated that users were permitted to "use, print out, save on a retrieval system, and otherwise copy and distribute" the reference for noncommercial use. *'552 Decision*; 2020 WL 402817, at *9–10 (citing J.A. 1429); *'713 Decision*, 2020 WL 402317, at *4 (same). Further, Centripetal presented no evidence to the Board showing that—despite the CD-ROM distribution—an interested person using reasonable diligence would not have been able to access Sourcefire either by purchasing the product or by receiving a copy of the user guide from another customer. *See '552 Decision*, 2020 WL 402817, at *10. Substantial evidence, including advertisements, reviews, and testimony from a Sourcefire company employee, supports the Board's finding that those interested and of skill in the art *actually* purchased Sourcefire. *Id.* at *11; *see also* J.A. 822. In sum, the large number of Sourcefire product customers, the number of years the product was available, the advertisements targeting those interested and of skill in the art, and the lack of confidentiality restrictions on copying or distributing Sourcefire support a finding of public accessibility. *See GoPro*, 908 F.3d at 694.

The Board properly rejected Centripetal's argument that *In re Bayer*, 568 F.2d 1357 (CCPA 1978), and *Medtronic, Inc. v. Barry*, 891 F.3d 1368 (Fed. Cir. 2018), require a different result. *'552 Decision*, 2020 WL 402817, at *11–12. In *Bayer*, we held that actual dissemination of a student's thesis to members of a graduate committee did not render the thesis publicly accessible. 568 F.2d at 1361–62. We recently explained in *Samsung* that the student's

---

actually disseminated without restriction to at least six persons").

thesis in *Bayer* was not publicly accessible because "the only people who kn[e]w how to find it [were] the ones who created it," and thus it could not be obtained with reasonable diligence by those interested and of skill in the art. *Samsung*, 929 F.3d at 1371–72. Here, in contrast, Sourcefire was publicly advertised and obtained by at least 586 customers.

In *Medtronic*, a video relating to spinal surgery was distributed at three separate meetings (two for surgeons, one for a private organization), and slides were distributed at two of the meetings. 891 F.3d at 1379. After the Board found lack of public accessibility of either the video or the slides, without distinguishing between the open and the closed meetings, or whether there was an expectation of confidentiality, we vacated and remanded. *Id.* at 1382–83. We instructed the Board to consider the "size and nature of the meetings," as well as whether an "expectation of confidentiality" existed, noting that these are "important considerations" in assessing public accessibility. *Id.* at 1382. In this case, the Board did exactly that. Far from finding Sourcefire to be a printed publication merely because the CD-ROMs were actually distributed to customers, the Board considered the size and nature of the group receiving the CD-ROMs and the absence of confidentiality restrictions. *'552 Decision*, 2020 WL 402817, at *10–12.

Contrary to Centripetal's contention, the Board's conclusion regarding public accessibility is not undermined by the fact that, unlike some of the cases, this case does not involve "free distribution of academic documents to conference and meeting attendees whose express purpose for attending the conference was to hear lectures regarding those same documents." Centripetal Opening Br. 18–19 (cleaned up). Public accessibility is not limited to circumstances of free or academic distributions; "commercial distribution" can qualify. *Garrett Corp. v. United States*, 422 F.2d 874, 877–78 (Ct. Cl. 1970) (distribution of 80 copies of a government report, including 6 to commercial companies,

constituted a printed publication because the report was "unclassified and unrestricted in its use"). The Board also reasonably found that Centripetal had not shown the cost of Sourcefire—which it found ranged from $1,385 to £25,000, *'552 Decision*, 2020 WL 402817, at *12 n.9; *see also* J.A. 4695, 4700—to be prohibitive to those interested and of skill in the art, given, *e.g.*, the evidence that at least 586 customers, at least some of them relevant artisans, purchased the product, *'552 Decision*, 2020 WL 402817, at *12; *'713 Decision*, 2020 WL 402317, at *5.

On this record, we agree with the Board that Sourcefire was publicly accessible and therefore qualifies as a printed publication.

B

We reject Centripetal's challenges to the Board's obviousness determination.

1

The Board found that Sourcefire teaches what is required by the determination claims. Centripetal argues otherwise by pointing to language in Sourcefire stating that the preprocessor "collects and reassembles all the packets" and inspects the stream as a "single, reassembled entity" rather than as "individual packets." J.A. 2064–65; *see also* Centripetal Opening Br. 22. This argument does not undermine the Board's finding.

As the Board reasoned, *how* Sourcefire obtains TLS-version values is irrelevant to the claims' scope. *'552 Decision*, 2020 WL 402817, at *17–18, *'713 Decision*, 2020 WL 402317, at *8. The claims in the '552 and '713 patents do not require that each individual packet is inspected for the TLS-version value, but only that a determination is made as to what that value is. *See* '552 patent, col. 11, lines 5–35 (claims require "a determination . . . 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"); '713 patent, col. 11, lines 8–25 (claims require "a determination . . . that [a packet received first or a packet received second] comprises data corresponding to a transport layer security TLS-version value").

Further, Centripetal's expert, Dr. Orso, acknowledged that the TLS-version value in a reassembled handshake is virtually always identical to the value for the individual packets associated with that handshake. J.A. 4647–48 (171:6–174:16). And substantial evidence established that relevant artisans would have understood that the TLS-version value is found in the first packet of a message. J.A. 809–10; J.A. 4653. Thus, the Board reasonably found that Sourcefire teaches determining this exact value because the information it obtains from the handshake will be identical to the first packet's header. *See* J.A. 2252 ("The SSL preprocessor extracts state and version information from specific handshake fields. Two fields within the handshake indicate the version of SSL or TLS used to encrypt the session and the stage of the handshake."). Substantial evidence thus supports the Board's finding that Sourcefire teaches the "determination" limitations of the patent claims.

2

Centripetal argues that the Board erred by finding a motivation to modify Sourcefire based on "common sense," Centripetal Opening Br. 24–27, and by not properly considering objective indicia of nonobviousness that negate any motivation a relevant artisan would have had to modify Sourcefire, *id.* at 27–31.

Centripetal's motivation argument substantially overlaps with its arguments that Sourcefire does not teach the "determination" limitations required by the claims. Specifically, Centripetal argues that the Board found that a relevant artisan would have been motivated to modify Sourcefire to include the "missing" claim limitations—the

"determination" limitations—and that such a finding was error because Sourcefire makes determinations from a reassembled packet stream, and a relevant artisan would not be motivated to modify that system to inspect individual packets. Centripetal Opening Br. 24–27. But the Board did not find that these limitations were "missing"; it found that Sourcefire taught the "determination" limitations because such limitations were not limited to systems that inspect individual packets. *See '552 Decision*, 2020 WL 402817, at *17–19; *'713 Decision*, 2020 WL 402317, at *8. And, as discussed above, nothing in either patent's claims requires individual packets to be inspected in order to determine their TLS-version value.

We also reject Centripetal's argument that the Board failed to properly weigh objective indicia of nonobviousness (specifically, long-felt but unmet need, industry praise, and commercial success/licensing). "In order to accord substantial weight to secondary considerations in an obviousness analysis, 'the evidence of secondary considerations must have a "nexus" to the claims, *i.e.*, there must be "a legally and factually sufficient connection" between the evidence and the patented invention.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019) (citing *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988)).

Here, Centripetal presented several articles praising its RuleGATE product as evidence of industry praise and long-felt but unmet need, including a paper (the ESG paper), J.A. 6900–08, and a Gartner article, J.A. 6909–18. But the RuleGATE product contains far more than what is claimed in the patent claims at issue here. And as the Board found, nothing in those articles ties the praise of RuleGATE, its alleged filling of an unmet need, or its success to the limitations in the claims. *See '552 Decision*, 2020 WL 402817, at *22–24; *'713 Decision*, 2020 WL 402317, at *10–12; *see also Polaris*, 882 F.3d at 1072.

Indeed, Centripetal's expert did not even create a claim-construction chart to map the products to each limitation. J.A. 4615–16. On this record, we agree with the Board that the objective indicia of nonobviousness were not entitled to substantial weight.

3

Finally, Centripetal challenges the Board's finding that Sourcefire teaches the operator required by the '552 patent. Centripetal argues that Sourcefire relies on "Snort rules" that include a "Rule Header" with a single specified "rule action" that can be taken only "'if the packet data matches all the conditions specified in a rule.'" Centripetal Opening Br. 32–33 (quoting J.A. 2188). For that reason, Centripetal urges, Sourcefire cannot disclose the required operator because its rules cannot "apply different packet transformation functions for different TLS-version values." *Id.*

But the '552 patent's claims do not require that a rule provide for more than one action. *See*, *e.g.*, '552 patent, col. 11, lines 5–35. Moreover, even under Centripetal's construction of "operator," the Board found, Sourcefire teaches an operator that meets both criteria required by that construction—that is, Sourcefire (1) determines "application-header-field-value criteria" through its keyword function (*e.g.*, identifies the packets' TLS-version value) and (2) applies a "packet transformation function" by using its Rule Action function to either block, alert, or allow packets matching the application-header-field-value criteria corresponding to the rule. *'552 Decision*, 2020 WL 402817, at *19–21; J.A. 2189–92, 2196. The language of the claims and of Sourcefire provide substantial evidence for the Board's finding that Sourcefire teaches the operator in the '552 patent's claims.

III

We have considered the remainder of Centripetal's arguments and find them to be unpersuasive.

For the foregoing reasons, the decisions of the Patent Trial and Appeal Board in IPR-1436 and IPR-1437 are affirmed.

AFFIRMED