Trials@uspto.gov
571-272-7822

Paper No. 42
Entered: June 9, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

RIVERBED TECHNOLOGY, INC.,
Petitioner,

v.

SILVER PEAK SYSTEMS, INC.,
Patent Owner.

Case IPR2014-00245
Patent 8,392,684 B2

Before DENISE M. POTHIER, JUSTIN T. ARBES, and HYUN J. JUNG, *Administrative Patent Judges.*

JUNG, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Riverbed Technology, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) on December 11, 2013 requesting institution of an *inter partes* review of claims 1–24 of U.S. Patent No. 8,392,684 B2 (“the ’684 patent”) pursuant to 35 U.S.C. §§ 311–19. Silver Peak Systems, Inc. (“Patent Owner”) did not file a preliminary response. Based on the Petition, we instituted *inter partes* review of claims 1–24. Paper 12 (“Dec. on Inst.”).

After institution, Patent Owner did not file a Patent Owner Response, and instead filed a Motion to Amend (Paper 16, “Mot.”) seeking to cancel claims 1–24 and substitute claims 25–48 in their place. Petitioner filed an Opposition (Paper 23, “Opp.”) to the Motion to Amend, and Patent Owner filed a Reply (Paper 26, “Reply”). In addition, the parties rely upon testimony from various declarants. Petitioner proffered the Declaration of Steven W. Landauer (Ex. 1008) with the Petition. Patent Owner proffered the Declaration of Geoff Kuenning, Ph.D. (Ex. 2001, “Kuenning Decl.”) with its Motion to Amend and a Second Declaration of Dr. Kuenning (Ex. 2013, “2d Kuenning Decl.”) with its Reply. In addition, a transcript of Dr. Kuenning’s deposition (Ex. 1010, “Kuenning Dep.”) was submitted by Petitioner. No deposition transcript was filed for Mr. Landauer.

An oral hearing in this proceeding was held on February 5, 2015, and a transcript of the hearing is included in the record (Paper 41, “Tr.”).

We have jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we grant Patent Owner’s Motion to Amend to the extent that it requests to cancel claims 1–24 of the ’684 patent. We determine that Patent Owner has not met its burden with respect to proposed substitute claims 25–48 and thus, the Motion is denied as to the substitute claims. The Motion to Amend, therefore, is *granted-in-part*.

A. The ’684 Patent (Ex. 1001)

The ’684 patent, titled “Data Encryption in a Network Memory Architecture for Providing Data Based on Local Accessibility,” issued on March 5, 2013 from U.S. Patent Application No. 11/497,026 (“the ’026 application”) filed on July 31, 2006. The ’026 application is a continuation-in-part of U.S. Patent Application No. 11/202,697, which issued as U.S. Patent No. 8,370,583 B2, which was the subject of IPR2013-00403.

The ’684 patent relates to encrypting data in a network memory architecture. Ex. 1001, 1:18. Figure 3 of the ’684 patent is reproduced below:

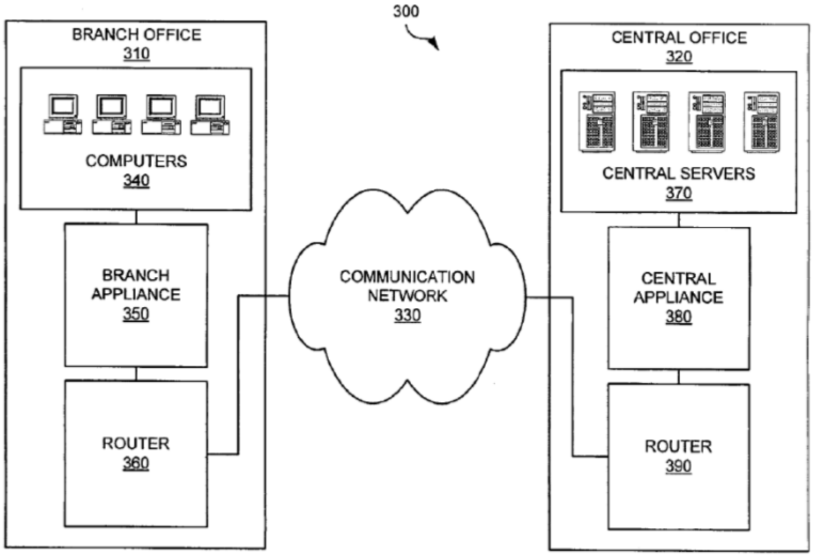

Figure 3 illustrates an exemplary implementation of network memory system 300. *Id.* at 4:62–63, 5:64–65. Network memory system 300 includes branch office 310 and central office 320. *Id.* at 5:65–66. Branch office 310 has computers 340 and branch appliance 350, and branch office 310 is coupled through router 360 to communication network 330. *Id.* at 5:66–6:2, 4–7. Branch appliance 350 "comprises hardware and/or software elements configured to receive data (e.g., email, files, and database[] transactions), determine whether a portion of the data is locally accessible to an appliance (e.g., central appliance **380**), generate an instruction based on the determination, and transfer the instruction to the appliance." *Id.* at 6:38–43.

Central office 320 includes central appliance 380 that is coupled to communication network 330 through router 390. *Id.* at 6:2–3, 7–10. Central appliance 380 "comprises hardware and/or software elements configured to receive data, determine whether a portion of the data is locally accessible to an appliance (e.g., the branch appliance **350**), generate an instruction based on the determination, and transfer the instruction to the appliance." *Id.* at 7:13–18. "In some embodiments, the instruction indicates an index within a database for storing and retrieving the data." *Id.* at 7:10–12.

In the exemplary embodiment, branch appliance 350 and central appliance 380 intercept network traffic between computers 340 and central servers 370. *Id.* at 7:29–32. Branch appliance 350 encrypts data, stores the encrypted data within a local copy in branch appliance 350, and transmits data to central appliance 380. *Id.* at 8:24–27. Branch appliance 350 also retrieves encrypted response data from the local copy per an instruction from central appliance 380, decrypts the response data, and forwards the response data to computers 340. *Id.* at 8:27–31.

Central appliance 380 also can receive an instruction from branch appliance 350 to store encrypted data in a local copy locally accessible to central servers 370. *Id.* at 8:34–37. Central appliance 380 is configured to determine whether the data is locally accessible to branch appliance 350 and to decrypt the data before transmitting the data to central server 370. *Id.* at 8:39–41, 43–45.

Figure 4 of the ’684 patent is reproduced below:

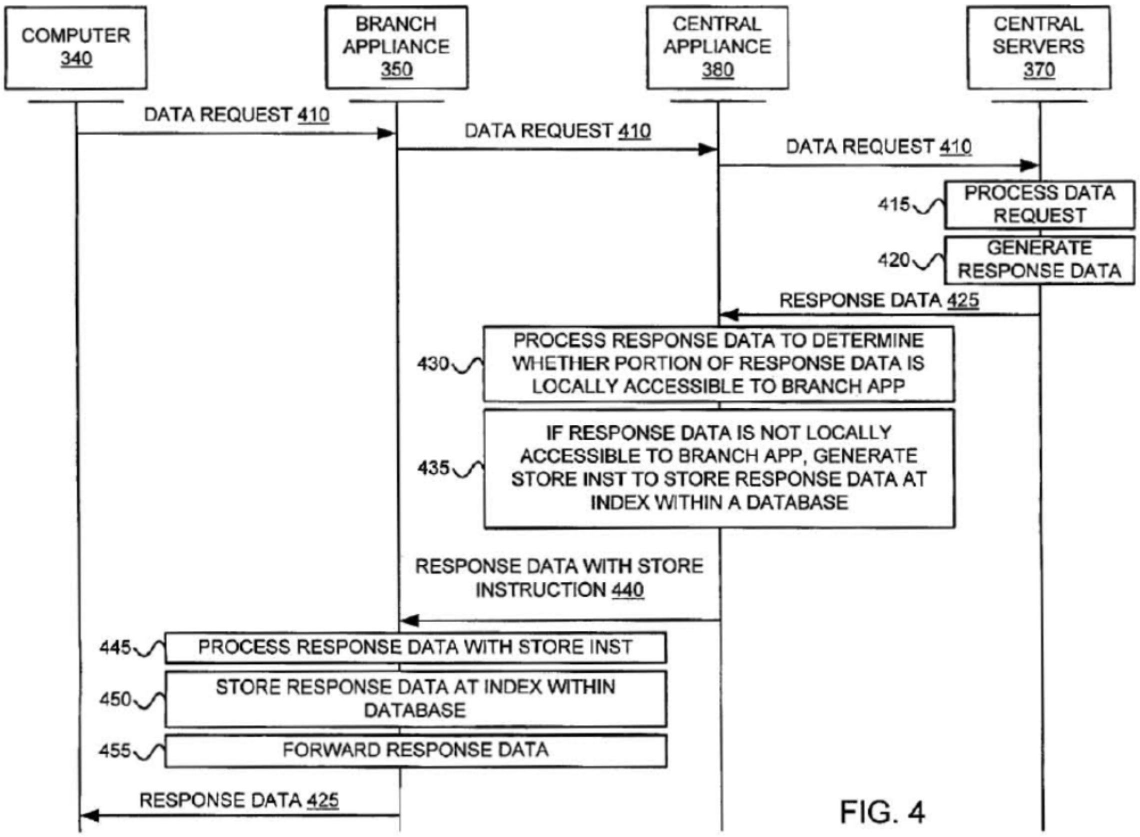
COMPUTER 340
BRANCH APPLIANCE 350
CENTRAL APPLIANCE 380
CENTRAL SERVERS 370
DATA REQUEST 410
DATA REQUEST 410
DATA REQUEST 410
415
PROCESS DATA REQUEST
420
GENERATE RESPONSE DATA
RESPONSE DATA 425
430
PROCESS RESPONSE DATA TO DETERMINE WHETHER PORTION OF RESPONSE DATA IS LOCALLY ACCESSIBLE TO BRANCH APP
435
IF RESPONSE DATA IS NOT LOCALLY ACCESSIBLE TO BRANCH APP, GENERATE STORE INST TO STORE RESPONSE DATA AT INDEX WITHIN A DATABASE
RESPONSE DATA WITH STORE INSTRUCTION 440
445
PROCESS RESPONSE DATA WITH STORE INST
450
STORE RESPONSE DATA AT INDEX WITHIN DATABASE
455
FORWARD RESPONSE DATA
RESPONSE DATA 425

FIG. 4

Figure 4 is a sequence chart for the network memory system where a response to a data request is not accessible locally to a branch device. *Id.* at 4:64–67, 9:25–28.

Computer 340 transmits data request 410 through branch appliance 350 and central appliance 380 to central server 370. *Id.* at 9:25–31. Central servers 370 generate response data 425 based on data request 410 and transmit response data 425 to central appliance 380. *Id.* at 9:34–36, 39–41, Fig. 4 (sequence 420). Central appliance 380 processes response data 425 to determine whether a portion of response data 425 is accessible locally to branch appliance 350. *Id.* at 9:45–47, Fig. 4 (sequence 430). If central appliance 380 determines that response data 425 is not accessible locally to branch appliance 350, central appliance 380 generates store instruction 440 and attaches store instruction 440 to response data 425. *Id.* at 11:41–48, Fig. 4 (sequence 435). However, if central appliance 350 determines that response data is available locally to branch appliance 350, central appliance 380 generates retrieve instruction 640 that indicates to branch appliance 350 to retrieve the response data at an index within a database. *Id.* at 12:27–31, Fig. 6.

In another embodiment, computer 340 transmits data request 710 through central appliance 380. *Id.* at 12:52–54, Fig. 7A. Central appliance 380 processes response data 725 to determine whether a portion of that data is locally accessible to branch appliance 350. *Id.* at 12:59–62, Fig. 7A (sequence 730). Central appliance 380 encrypts flow history pages 545 that include pages, page state information, and data, and "will transmit the deltas (i.e., the portion of the response data **725** that is not locally accessible) to the branch appliance **350**." *Id.* at 9:51–63, 13:11–15. Central appliance 380 can generate a store instruction that "indicates to the branch appliance **350** to store the deltas at an index within the database." *Id.* at 13:20–22. Branch appliance 350 stores the deltas in accordance with the store instruction. *Id.* at 13:42–45. "If the deltas are not encrypted, the branch appliance **350** further encrypts the deltas." *Id.* at 13:45–47.

If retrieve instruction 640 is smaller in size than response data 625, central appliance 380 transmits only retrieve instruction 640, but if retrieve instruction 640 is larger than response data 625, central appliance 380 transmits response data 625 instead. *Id.* at 12:32–33, 35-39. Thus, according to the ’684 patent, central appliance 380 optimizes network traffic over communication network 330. *Id.* at 12:33–35.

B. Status of the Claims

The ’684 patent has 24 claims, all of which are challenged. Claims 1–7 recite a network memory system; claims 8–14 recite a method; and claims 15–24 recite a software product. Claim 1, for example, recites:

> 1. A network memory system for ensuring compliance, comprising:
>
> a source-site appliance comprising a first processor and a first memory device, and configured to be coupled to a source-site computer via a source-site local area network;
>
> a destination-site appliance comprising a second processor and a second memory device, and configured to be coupled to a destination-site computer via a destination-site local area network, the source-site computer in communication with the destination-site computer via a wide area network;
>
> the source-site appliance configured to intercept data sent from the source-site computer to the destination-site computer, encrypt the data, store the data in the first memory device, determine whether the data exists in the second memory device, and transmit a store instruction comprising the data if the data does not exist in the second memory device; and
>
> the destination-site appliance configured to receive the store instruction from the source-site appliance, store the data in the second memory device, subsequently receive a retrieve instruction comprising an index at which the data is stored in the second memory device, process the retrieve instruction to obtain encrypted response data, and decrypt the encrypted response data.

In its Motion to Amend, Patent Owner proposes a substitute claim for each of the challenged claims. Mot. 1–7. Proposed substitute claim 25 recites, with underlined material indicating language added to original patent claim 1:

> 25. A network memory system for ensuring compliance, comprising:
>
> a source-site appliance comprising a first processor and a first memory device, and configured to be coupled to a source-site computer via a source-site local area network;
>
> a destination-site appliance comprising a second processor and a second memory device, and configured to be coupled to a destination-site computer via a destination-site local area network, the source-site computer in communication with the destination-site computer via a wide area network;
>
> the source-site appliance configured to intercept original data sent from the source-site computer to the destination-site computer, encrypt the original data to generate encrypted data, store the encrypted data in the first memory device, determine whether a representation of the original data exists in the second memory device, and transmit a store instruction comprising the original data if the representation of the original data does not exist in the second memory device; and
>
> the destination-site appliance configured to receive the store instruction from the source-site appliance, encrypt the original data received with the store instruction at the destination-site appliance to generate encrypted received data, store the encrypted received data in the second memory device, subsequently receive a retrieve instruction comprising an index at which the encrypted received data is stored in the second memory device, process the retrieve instruction to obtain encrypted response data comprising at least a portion of the encrypted received data, and decrypt the encrypted response data.

Mot. 1–2.

C. The Asserted Grounds of Unpatentability

We instituted the instant *inter partes* review on the following grounds of unpatentability.

Reference[s]	**Basis**	**Claims challenged**
McCanne[1]	§ 102	1, 2, 7–9, 14–16, and 21–24
McCanne and Stein[2]	§ 103	3, 10, and 17
McCanne and Rarick[3]	§ 103	4, 11, and 18
McCanne and Anand[4]	§ 103	5, 12, and 19
McCanne and Gleichauf[5]	§ 103	6, 13, and 20

Dec. on Inst. 24–25.

II. ANALYSIS

A. Challenged Claims

As noted above, Patent Owner did not file a Patent Owner Response to the Petition. In its Motion to Amend, Patent Owner "moves to cancel claims 1–24 and to substitute claims 25–48 in their place." Mot. 1; *see* 35 U.S.C. § 316(d); 37 C.F.R. § 42.121(a)(3) ("A motion to amend may cancel a challenged claim or propose a reasonable number of substitute claims."). Patent Owner's request to cancel claims 1–24 is not contingent on the claims being determined to be unpatentable. We grant the request and turn to the proposed substitute claims in the Motion to Amend.

[1] U.S. Patent Application Publication No. 2004/0088376 A1, published May 6, 2004 (Ex. 1003).

[2] U.S. Patent Application Publication No. 2003/0133568 A1, published July 17, 2003 (Ex. 1004).

[3] U.S. Patent Application Publication No. 2004/0086114 A1, published May 6, 2004 (Ex. 1005).

[4] U.S. Patent Application Publication No. 2003/0002664 A1, published Jan. 2, 2003 (Ex. 1006).

[5] U.S. Patent Application Publication No. 2003/0149869 A1, published Aug. 7, 2003 (Ex. 1007).

B. Proposed Substitute Claims

As the moving party, Patent Owner bears the burden of proof to establish that it is entitled to the relief requested. *See* 37 C.F.R. § 42.20(c). Entry of proposed amendments is not automatic, but occurs only upon the patent owner having met the requirements of 37 C.F.R. § 42.121 and demonstrated, by a preponderance of the evidence, the patentability of the proposed substitute claims. *See Idle Free Sys., Inc. v. Bergstrom, Inc.*, Case IPR2012-00027, slip op. at 7–8 (PTAB June 11, 2013) (Paper 26, "*Idle Free*") (informative); *Toyota Motor Corp. v. American Vehicular Scis. LLC,* Case IPR2013-00419, slip. op. at 4–5 (PTAB Mar. 7, 2014) (Paper 32, "*Toyota*"). For the reasons explained below, we conclude that Patent Owner has not met its burden with respect to claims 25–48.

1. Claim Construction

Patent Owner bears the burden in a motion to amend to show a patentable distinction of each proposed substitute claim over the prior art. *See* 37 C.F.R. § 42.20(c). Accordingly, a "patent owner should identify specifically the feature or features added to each substitute claim, as compared to the challenged claim it replaces, and come forward with technical facts and reasoning about those feature(s)." *Idle Free* at 7. This includes "construction of new claim terms, sufficient to persuade the Board that the proposed substitute claim is patentable over the prior art of record, and over prior art not of record but known to the patent owner." *Id.*; *Toyota* at 5. Further, consistent with the statute and legislative history of the Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284 (2011), the Board interprets claims using the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R.

§ 42.100(b); *In re Cuozzo Speed Tech., LLC*, 778 F.3d 1271, 1279–83 (Fed. Cir. 2015).

In the Decision on Institution, we interpreted various claim terms of the independent claims of the ’684 patent as follows.

Term	**Interpretation**
“network memory”	“device(s) in a network for storing information”
“appliance”	“hardware and/or software elements applied to a particular use”
“instruction”	“a message or signal that indicates, explicitly or implicitly, an action to perform”

See Dec. on Inst. 7–11. The parties do not dispute these interpretations in their papers. We do not perceive any reason or evidence that now compels any deviation from these interpretations. Accordingly, for purposes of assessing the proposed substitute claims, we incorporate our previous analysis. *See id.*

Patent Owner’s proposed substitute claims add limitations to the original independent claims of the ’684 patent, and in its Motion to Amend, Patent Owner states it “does not believe any terms of the proposed substitute claims require construction because there are no new terms, the meaning of which reasonably can be anticipated as subject to dispute.” Mot. 1–8.

We determine, however, that for purposes of assessing the proposed substitute claims, the term “data” needs interpretation. Petitioner argues that original claim 1 requires the source-site appliance to encrypt data before it is sent and Patent Owner’s proposed substitute claims eliminate this feature, thereby enlarging the scope of the claims. Opp. 1–4. Original claim 1 recites, *inter alia*, “the source-site appliance configured to . . . transmit a store instruction comprising the data if the data does not exist in the second memory device; and the destination-site appliance configured to receive the store instruction from the source-site appliance.” Original claim 1 also recites that the source-site appliance is “configured to intercept data sent from the source-site computer to the destination-site computer, encrypt the data, store the data in the first memory device, [and] determine whether the data exists in the second memory device.” Although claim 1 recites “encrypt the data” before “transmit a store instruction comprising the data,” the language of claim 1 does not require explicitly, as a matter of timing, that the data is encrypted before it is transmitted as part of the store instruction. *See* 2d Kuenning Decl. ¶¶ 6, 8. As Patent Owner points out, the Specification of the ’684 patent supports interpreting “data” as unencrypted data, and that the claims are broad enough to encompass any order. Reply 1; Tr. 10:11–17:18; 2d Kuenning Decl. ¶¶ 4–9.

Patent Owner cites column 13, lines 45–47, of the ’684 patent, which is part of a description of an embodiment illustrated in Figures 7A and 7B. *See* Ex. 1001, 12:48–13:48; Reply 1. In that embodiment, the ’684 patent describes that central appliance 380 processes response data 725 to determine whether a portion of that data is locally accessible to branch appliance 350 and “will transmit the deltas (i.e., the portion of the response data **725** that is not locally accessible) to the branch appliance **350**.” *Id.* at 12:59–62, 13:11–15. The ’684 patent also states that “[i]f the deltas are not encrypted, the branch appliance **350** further encrypts the deltas.” *Id.* at 13:45–47. Thus, the ’684 describes an embodiment where data can be, but need not be, encrypted before it is transmitted as part of the store instruction.

As discussed above, the claims do not require encrypting data before transmitting that data as part of the store instruction. Accordingly, we decline to import into the claims a limitation based on a specific embodiment in the Specification. *See, e.g., SuperGuide Corp. v. DirecTV Enters., Inc.,* 358 F.3d 870, 875 (Fed. Cir. 2004) ("[A] particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment."). We decline to read the exemplary disclosure of encrypting the data before transmitting it with the store instruction into the broadest reasonable interpretation of "data."

Moreover, original claim 8 recites a method including the steps of "encrypting the data" and "transmitting a store instruction comprising the data." Determining if the steps of a method claim that do not otherwise recite an order, must be performed nonetheless in the order in which they are written involves a two-part test. "First, we look to the claim language to determine if, as a matter of logic or grammar, they must be performed in the order written. If not, we next look to the rest of the Specification to determine whether it 'directly or implicitly requires such a narrow construction.' . . . If not, the sequence in which such steps are written is not a requirement." *Altiris, Inc. v. Symantec Corp*. 318 F.3d 1363, 1369–70 (Fed. Cir. 2003) (citation omitted); *see also Loral Fairchild Corp. v. Sony Corp*., 181 F.3d 1313, 1321 (Fed. Cir. 1999) (holding that the claim language itself indicated that the steps had to be performed in their written order because the second step required the alignment of a second structure with a first structure formed by the prior step); *Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc*., 152 F.3d 1368, 1375–76 (Fed. Cir. 1998) (holding that the steps of a method claim had to be performed in their written order because each subsequent step referenced something logically indicating the prior step had been performed).

First, the language of claim 8 does not compel that the step of "encrypting the data" must be performed before the step of "transmitting a store instruction comprising the data" as a matter of logic or grammar. Claim 8 recites, *inter alia*, "intercepting data," "encrypting the data," "storing the data," and "transmitting a store instruction comprising the data." Although the later recited steps refer to "the data," neither logic nor grammar compels finding a particular order of performing these later steps. For example, the transmitting step could be performed before the encrypting and storing steps.

Turning to whether the Specification of the '684 patent directly or implicitly requires a narrower construction in which the recited steps are performed in a particular order, Patent Owner cites a portion of the '684 patent that describes an embodiment illustrated in Figures 7A and 7B. As discussed above, the '684 patent states that "[i]f the deltas are not encrypted, the branch appliance **350** further encrypts the deltas." Ex. 1001, 13:45–47. Thus, the '684 patent describes an embodiment where data can be, but need not be, encrypted before it is transmitted as part of the store instruction. In the context of this description, we determine that the Specification of the '684 patent does not require construing "data" in claim 8's "transmitting a store instruction comprising the data" to be "encrypted data."

For the foregoing reasons, we interpret "data" in the original claims of the '684 patent to be "encrypted or unencrypted data." The proposed substitute claims include two modifiers for the term "data." For example, proposed substitute claim 25 recites "encrypt[ing] the original data to generate encrypted data." Thus, the plain meaning of the proposed substitute claims is that the "original data" is unencrypted and the "encrypted data" is encrypted. *See* Tr. 13:6–10.

2. No Broadening of Scope

Proposed substitute claims in an *inter partes* review "may not enlarge the scope of the claims of the patent." 35 U.S.C. § 316(d)(3); *see* 37 C.F.R. § 42.121(a)(2)(ii). In its Motion to Amend, Patent Owner proposes substituting one of claims 25–48 for one of claims 1–24. Mot. 1–7. Each claim includes all the limitations of the corresponding claim for which it is a substitute, and adds additional limitations. Proposed substitute claims 25, 27–29, 31, 32, 39, 41–43, and 45 recite "original data," and proposed substitute claims 34–36 recite "~~first~~ original data."

Petitioner argues that "original claim 1 of the '684 patent requires that 'the data' transmitted by the source-site appliance to the destination-site appliance be in encrypted form" and that proposed substitute claim 25 enlarges the scope of claim 1 because "the data flowing between the two appliances **is *not* encrypted**." Opp. 1–3; *see also* Tr. 34:5–44:19 (presenting similar arguments). Patent Owner replies that the original claims "do not require that 'the data' transmitted by the source-site appliance is encrypted." Reply 1 (citing 2d Kuenning Decl.[6] ¶¶ 4–12). Patent Owner also argues that the Specification of the '684 patent describes embodiments in which transmitted data is unencrypted. *Id.* (citing Ex. 1001, 13:45–47; 2d Kuenning Decl. ¶¶ 6, 8, 12); Tr. 10:11–17:18. For the reasons discussed above, we interpret "data" in the original claims to be "encrypted or

[6] *See* Paper 28 (Order renumbering Ex. 2007 as Ex. 2013).

unencrypted data." Thus, we are not persuaded by Petitioner's arguments that proposed substitute claim 25 enlarges the scope of claim 1, for which claim 25 is a proposed substitute.

Petitioner also argues that proposed substitute claim 38 enlarges the scope of claim 14, which claim 38 is proposed to replace. Opp. 4; Paper 30. As issued, claim 14 depends from claim 9. Ex. 1001, 18:61–63. Proposed substitute claim 38 depends from proposed substitute claim 32, which is proposed to replace claim 8. Mot. 3. In other words, the dependency of proposed substitute claim 38 has changed. Patent Owner replies that "[a]lthough the '684 patent shows claim 14 depending from original claim 9, this dependency is a printing error." Reply 1; *see also* Paper 29 (arguing that the dependency of claim 14 is a printing error). Patent Owner also filed a request for certificate of correction. Exs. 3001, 3002; *see also* Paper 34 (granting Patent Owner's motion for authorization to file a certificate of correction). A certificate of correction for the '684 patent issued during this proceeding and states that the '684 patent is corrected so that "[i]ssued claim 14 should depend from issued claim 8." Ex. 3003. In view of the certificate of correction issued for the '684 patent, Petitioner's argument that proposed substitute claim 38 enlarges the scope of claim 14 is not persuasive.

Accordingly, for the foregoing reasons, we determine that the proposed substitute claims do not enlarge the scope of the original patent claims.

3. Written Description Support

Pursuant to 37 C.F.R. § 42.121(b), a motion to amend in an *inter partes* review must set forth "[t]he support in the original disclosure of the patent for each claim that is added or amended" and "[t]he support in an earlier-filed disclosure for each claim for which benefit of the filing date of the earlier filed disclosure is sought."

In its Motion to Amend, Patent Owner explains how the subject matter of its proposed substitute claims have written description support in the Specification of the '026 application, which issued as the '684 patent. Mot. 8–9. Regarding the added limitations, Patent Owner relies on Figures 4, 6, and 7 and paragraphs 56–58, 66–71, and 76 of the '026 application. *Id.* Patent Owner states that the cited portions describe "store and retrieve operations including encrypting flow history pages (FHPs) at the source-site appliance using AES, DES, 3DES," "that the destination-site appliance can encrypt received data," and "decrypting encrypted response data and transmitting the decrypted response data." *Id.* Patent Owner also provides citations for other limitations of the proposed substitute claims. *Id.* (citing ¶¶ 39–49, 79–81, 94–96; Figs. 3, 8, 9, 12, 13 of the '026 application). Petitioner in its Opposition does not argue that the claims lack sufficient written description support.

Upon review of Patent Owner's arguments and the disclosures of the application that issued as the '684 patent, we conclude that Patent Owner has made a sufficient showing that proposed claims 25–48, as a whole, have written description support in the disclosure of the application as filed.

4. Proposed Substitute Claims

Having interpreted the language of the claims and having determined that Patent Owner's proposed substitute claims do not enlarge the scope of the claims of the '684 patent and have sufficient written description support, we turn to the claims specifically to determine if Patent Owner has met its burden of proof.

In a motion to amend, the patent owner bears the burden of proof to demonstrate patentability of its proposed substitute claims over the prior art and, thus, entitlement to the claims. *Idle Free* at 7. This does not mean that the patent owner is assumed to be aware of every item of prior art known to a person of ordinary skill in the art. The patent owner, however, should explain in its motion why the proposed substitute claims are patentable over not just the prior art of record, but also prior art not of record but known to the patent owner:

> A patent owner should identify specifically the feature or features added to each substitute claim, as compared to the challenged claim it replaces, and come forward with technical facts and reasoning about those feature(s), including construction of new claim terms, sufficient to persuade the Board that the proposed substitute claim is patentable over the prior art of record, and over prior art not of record but known to the patent owner. The burden is not on the petitioner to show unpatentability, but on the patent owner to show patentable distinction over the prior art of record and also prior art known to the patent owner. Some representation should be made about the specific technical disclosure of the closest prior art known to the patent owner, and not just a conclusory remark that no prior art known to the patent owner renders obvious the proposed substitute claims.

Id. This includes addressing the basic knowledge and skill set possessed by a person of ordinary skill in the art even without reliance on any particular item of prior art. *Id.* at 7–8; *Toyota* at 4–5. The petitioner then has the opportunity, in its opposition, to argue any deficiency in the patent owner's motion and "come forward with specific evidence and reasoning, including citation and submission of any applicable prior art," to rebut the patent owner's position on patentability. *Idle Free* at 8.

Proposed substitute claim 25 adds that the source-site appliance is

> configured to intercept original data sent from the source-site computer to the destination-site computer, encrypt the original data to generate encrypted data, store the encrypted data in the first memory device, determine whether a representation of the original data exists in the second memory device, and transmit a store instruction comprising the original data if the representation of the original data does not exist.

Proposed substitute claim 25 also adds that the destination-site appliance is

> configured to . . . encrypt the original data received with the store instruction at the destination-site appliance to generate encrypted received data, store the encrypted received data in the second memory device, subsequently receive a retrieve instruction comprising an index at which the encrypted received data is stored . . . , [and] process the retrieve instruction to obtain encrypted response data comprising at least a portion of the encrypted received data.

Patent Owner asserts that the "prior art does not disclose or suggest the claimed feature of 'encrypt[ing] the original data received with the store instruction at the destination-site appliance to generate encrypted received data' and 'stor[ing] the encrypted received data in the second memory device.'" Mot. 9–10 (citing Kuenning Decl. ¶¶ 45–76). Patent Owner also states that "a system having the claimed features could be configured to independently encrypt . . . data stored at each source-site and each destination-site appliance," which "would enable appliances at different locations to meet their own specific compliance and/or performance requirements." *Id.* Patent Owner also states that "a system having the claimed features could be configured to independently encrypt data in transit and data in storage." *Id.* at 10–11 (citing Kuenning Decl. ¶ 22).

Patent Owner contends that McCanne "represents the closest prior art known to the Patent Owner." Mot. 11 (citing Kuenning Decl. ¶ 54).

a. McCanne

McCanne relates to systems for moving data efficiently through limited-bandwidth channels. Ex. 1003 ¶ 2. In networked-file systems, applications may use files stored in another location. *Id.* ¶ 4. An example of a transaction involving such files can include a client sending a request for the file to a server, and the server sending the file as a response to the client. *Id.* ¶¶ 43, 45. McCanne describes a networked client-server system 10, where such transactions can occur, as shown in Figure 1, reproduced below. *Id.* ¶ 48.

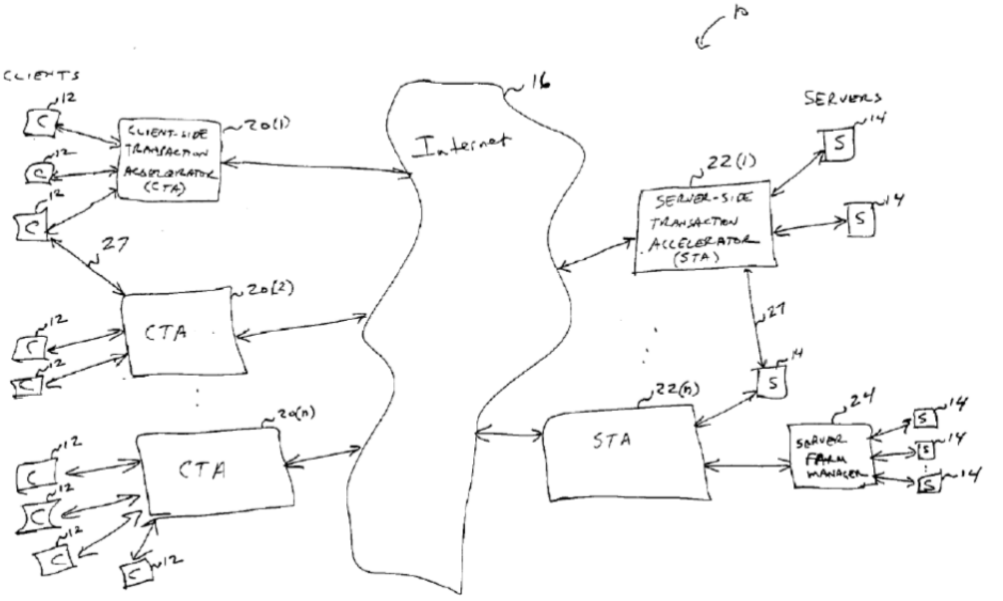

Figure 1 depicts clients 12 coupled to servers 14 over network 16 via client-side transaction accelerators 20 ("CTAs") and server-side transaction accelerators 22 ("STAs"). *Id.* The CTAs and STAs each may be implemented as a single program with data memory, program memory, and a processor. *Id.* ¶ 64. CTA 20 and STA 22 can each include a persistent segment store ("PSS"). *Id.* ¶ 61. McCanne describes that when client 12 sends a request for data, the request passes through CTA 20 and is routed to the appropriate STA 22. *Id*. ¶¶ 52, 56. Server 14 receives the request, formulates a response to the request, and sends the response toward the client 12 via STA 22 to which server 14 is coupled. *Id*. ¶ 57.

The STA examines the payload of the transaction and stores strings or other sequences of data (i.e., segment data) derived from those payloads. *Id*. ¶ 69. If the STA can expect that the CTA would have the segment data, the STA may replace the segment data in the payload with references to the segment data. *Id*. McCanne describes that the sending accelerator (the STA in the example above) determines "whether or not to replace the segment data with a reference" either because it appeared in an earlier transaction or was previously sent through other processes to the receiving accelerator (the CTA in the example above). *Id*. McCanne describes "a bindings table of a simple PSS" and "the bindings table stores a plurality of bindings." *Id.* ¶ 87. "The binding records might include other fields . . . such as those listed in Table 1." *Id.* Table 1 includes "encoding method identifier (e.g., unencoded raw data, run-length encoded, MD5, encoded, encrypted)." *Id.* Table 1. The sending transaction accelerator ("TA") can also "transmit invertible functions of the segments, e.g., forward correction encoded blocks of segments, encryptions of segments, signatures of segments, or the like." *Id.* ¶ 89.

The CTA that receives the reference to the segment data substitutes the reference with the segment data before sending the reconstructed file to the client that made the request. *Id*. ¶ 70. "By sending references instead of segment data, the total traffic between T[ransaction] A[ccelerators] during the transaction is reduced." *Id.* ¶ 75.

b. Patentability over McCanne

Patent Owner acknowledges that McCanne discloses encryption, but argues that McCanne "does not substantively discuss or contemplate data security or implementing policies for regulatory compliance through application data security to WAN optimization data." *Id.* (citing Kuenning Decl. ¶ 46; Ex. 1003 ¶¶ 87–89). Patent Owner also argues that McCanne "does not disclose performing encryption at the <u>receiving TA</u>, as recited in the proposed substitute claims." *Id.* (discussing Ex. 1003 ¶¶ 87–89). Patent Owner further argues that other prior art fails to disclose the recited encryption features. *Id.* at 11–12 (citing Kuenning Decl. ¶ 54).

Patent Owner asserts that the "proposed substitute claims are not rendered obvious in view of the prior art." Mot. 12 (citing Kuenning Decl. ¶ 50). Patent Owner argues that, at the time of invention, an ordinarily skilled artisan would have understood "data could be secured using encryption when it is being stored in files and that data could be secured using encryption when being transmitted between servers and clients" but "would not have appreciated the data security risks and vulnerabilities posed by WAN optimization devices." *Id.* (citing Kuenning Decl. ¶¶ 51–66). Patent Owner argues that "data security risks in the context of data stored at WAN optimization devices were generally unaddressed prior to the invention of the proposed substitute claims." *Id.*

Patent Owner argues that McCanne "mentions 'security' only in its 'Background' section in the context of very generally explaining that a conventional non-accelerated network configuration may include security measures to control access to servers" but "does not once mention data security in the context of describing its transaction accelerator system." Mot. 14 (citing Kuenning Decl. ¶¶ 69, 70). Patent Owner also argues that, although McCanne mentions that data can be stored encrypted, McCanne "does not teach that encryption is desirable for the purpose of securing data stored at the TAs." *Id.* Patent Owner further argues that the embodiment of McCanne, in which encryption-based encoding is applied, would have practical problems with "key management, distribution, and revocation and, increased risk of potentially catastrophic data breaches." *Id.* Patent Owner, thus, argues that McCanne "would not have led a person of ordinary skill in the art to the security features of the proposed substitute claims." *Id.* at 14–15 (citing Kuenning Decl. ¶ 75). Patent Owner further argues that McCanne "only teaches encoding of segments according to a reversible function (which may be encryption)" but a "person of ordinary skill in the art would have found it most efficient to perform such encoding only at the sending TA" because "it was much simpler, less expensive, and more efficient from a processing standpoint to encode the data only once at the sending TA instead of encoding at each receiving TA." *Id*. at 15.

Petitioner argues that McCanne anticipates proposed substitute claims 25, 26, 31–33, 38–40, and 45–48. Opp. 8–12. Petitioner asserts that McCanne discloses "the STA (***source-site appliance***) intercepts data (***original data***) sent from the server (***source-site computer***) to the client (***destination-site computer***)." *Id.* at 8–9 (citing Ex. 1003 ¶¶ 60, 69, 89, 94). Petitioner also contends that the STA encrypts the original data and stores the encrypted data in its persistent segment store ("PSS") or first memory device. *Id.* (citing Ex. 1003 ¶¶ 87–89, 94, 95, Table 1, claims 4, 5).

Petitioner further argues that the STA determines whether the original data exists in the PSS of a CTA or destination-site appliance. *Id.* (citing Ex. 1003 ¶¶ 69, 78, 90). Petitioner also argues that the STA transmits encoded data or a store instruction that includes the original data in the form of "bindings" to the CTA. *Id.* (citing Ex. 1003 ¶¶ 69, 78, 88, 90, 94, Table 1).

Petitioner argues that McCanne discloses that the CTA is configured to receive the encoded data or store instruction that includes original data. Opp. 9 (citing Ex. 1003 ¶¶ 78, 87–89, 94–97, 101, Table 1). Petitioner also argues that McCanne discloses encrypting the received data and storing the encrypted data in the PSS or second memory device of the CTA. *Id.* (citing Ex. 1003 ¶¶ 78, 87–89, 101, Table 1, claims 4, 5).

Petitioner argues that Patent Owner acknowledges that McCanne discloses disk encryption at the sending TA but incorrectly asserts that McCanne does not disclose encryption at the receiving TA. Opp. 10 (citing Mot. 10). Petitioner contends that Patent Owner's declarant acknowledges that either accelerator 20 or 22 can be a receiver, and both can store segment data. *Id.* at 11 (citing Kuenning Dep. 24–25). Petitioner also argues that McCanne discloses encrypting segment data when it is stored. *Id.* (citing Ex. 1003 ¶¶ 87–89, claims 4, 5). Petitioner, thus, argues McCanne discloses that the receiving TA stores data and that, when the data is stored, it is encrypted. *Id.* at 11–12 (citing Ex. 1003 ¶¶ 87–89, claims 4, 5).

Petitioner also argues that McCanne renders obvious proposed substitute claims 25, 26, 31–33, 38–40, and 45–48. Opp. 12–15. In particular, Petitioner argues that McCanne renders obvious modifying a receiving WAN optimization device to encrypt and store data. *Id.* at 12. Petitioner asserts that Patent Owner's declarant acknowledges McCanne discloses that the receiving WAN optimization device stores segment data, states that “encryption techniques could be used to secure it,” and states that it was known to skilled artisans to “‘implement disk encryption both on the sending side and the receiving side.’” *Id.* at 12–13 (citing Kuenning Dep. 7, 24–25; Kuenning Decl. ¶¶ 51, 58, 76). Petitioner also asserts that modifying McCanne “to encrypt data at both the sending and receiving side device would have been a predictable result,” the proposed modification addresses a concern of those skilled in the art regarding “security of data stored on WAN optimization devices,” and “as acknowledged by Patent Owner’s expert, it was known how to implement disk encryption on a receiving side device.” *Id.* at 14.

Patent Owner replies that “it would not have been obvious to apply encryption on a receiving side of a WAN optimization appliance.” Reply 4 (citing 2d Kuenning Decl. ¶¶ 40–43; Mot. 9–15). Patent Owner also argues that McCanne does not teach encrypting received data and storing the encrypted received data in the PSS of the CTA. *Id.* (citing 2d Kuenning Decl. ¶¶ 44–51). Patent Owner asserts that McCanne “exclusively contemplates performing encryption at a <u>sending</u> TA” because “[f]or any given transaction, only the sender, and not the receiver, may perform encryption.” *Id.* at 5. Patent Owner relies on its declarant’s testimony to argue that “it would <u>not</u> have been obvious to encrypt the data in an optimization appliance” and the Kuenning Declarations “explain why at length.” *Id.* (citing Kuenning Decl. ¶¶ 51–76; 2d Kuenning Decl. ¶¶ 52–54).

Patent Owner only disputes Petitioner’s assertion that McCanne discloses that the destination-site appliance is configured to “encrypt the original data received with the store instruction at the destination-site appliance to generate encrypted received data" and "store the encrypted received data in the second memory device," recited in proposed substitute claim 25 and similarly recited in the other proposed substitute independent claims. *See* Reply 4–5. We agree with Patent Owner that McCanne does not disclose explicitly that its receiving TA is configured to "encrypt the original data received with the store instruction . . . to generate encrypted received data" and "store the encrypted received data in the second memory device." *See id*. at 5. Thus, we are not persuaded that McCanne anticipates the proposed substitute claims, as asserted by Petitioner, because McCanne fails to describe each and every element as set forth in the proposed substitute claims, either expressly or inherently. *See* Opp. 8–12; *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

Patent Owner, however, has not shown sufficiently that the proposed substitute claims would not have been obvious over McCanne. McCanne discloses "a bindings table of a simple PSS" and "the bindings table stores a plurality of bindings." Ex. 1003 ¶ 87 (describing Fig. 3). McCanne also states that "[t]he binding records might include other fields . . . such as those listed in Table 1." *Id.* Table 1 includes "encoding method identifier (e.g., unencoded raw data, run-length encoded, MD5, encoded, *encrypted*)." Ex. 1003, Table 1 (emphasis added). Thus, in view of paragraph 87 and Table 1, McCanne teaches that the bindings table of its PSS stores data with a field that identifies the data encoding method by which the stored data is encoded, such as "encrypted." Also, as Petitioner points out (Opp. 11), McCanne claims "when segment data is to be stored as part of a segment reference, transforming the segment data via an invertible function of the segment data, and storing the results of this transformation" and "the invertible function is one or more of a forward error correction function, an *encryption* function, and a signature function." Ex. 1003, claims 4, 5 (emphasis added). Thus, claims 4 and 5 also teach, when segment data is to be stored, transforming the segment data via an encryption function and storing the results of the transformation.

McCanne also states that the "elements of CTA **20** . . . include . . . a persistent segment store (PSS) **36**." Ex. 1003 ¶ 61. As discussed above, the bindings table of a PSS stores a plurality of bindings and encoding method identifier, such as "encrypted." *See* Ex. 1003 ¶ 87, Table 1. McCanne further states that the "receiver can obtain the segment data for inclusion in its persistent store" and the "receiving TA can obtain segment data for storage in its PSS from a side channel or as part of the traffic from the sending TA." Ex. 1003 ¶¶ 73, 76. McCanne also states that "[a]t the receiving TA (the CTA . . .), . . . for the new, changed segments, the references are resolved from bindings included in the stream from the sender" and "[t]hose bindings can then be stored . . . into the receiver's PSS." *Id.* ¶ 78. As Petitioner points out (Opp. 9), McCanne further states "the sending TA *can* transmit invertible functions of the segments, e.g., forward error correction encoded blocks of segments, *encryptions of segments*, signature of segments, or the like." *Id.* ¶ 89 (emphases added). Thus, McCanne teaches that Petitioner's asserted destination-site appliance, the CTA, can store encrypted data in its PSS, the asserted second memory device, as Dr. Kuenning acknowledges. *See* Kuenning Dep. 24:15–25, 25:5–13. The testimony cited by Petitioner from the deposition of Dr. Kuenning is reproduced below:

> Q. Now, assuming a person in the field knew how to implement disk encryption, whether that was by writing an algorithm or using commercially available software, it would have been known to implement -- it would have been known how to implement disk encryption both on the sending side and the receiving side?
> A. The knowledge existed, yes.
> . . .
> Q. Both transaction accelerators, 20 and transaction accelerator 22 [in McCanne], has it's own storage medium; right?
> A. That's correct.
> Q. That storage medium is the persistent segment storage; right?
> A. Yes.
> Q. Or PSS; correct?
> A. Yes.
> Q. And those are marked by 36 and 46; correct?
> A. Yes.
> Q. Both sides store segmented data in it's respective PSS; correct?
> A. That's correct.

Kuenning Dep. 24:1–7, 24:15–25:7. Petitioner also cites the following from the deposition of Dr. Kuenning:

> Q. In 2005, it was known to those of ordinary skill in the art that there were benefits to encrypting data on both sending-side disks and receiving-side disks?
> A. It was generally known to people of ordinary skill in the art that in certain circumstances where data as at risk. Encryption was one of the solutions available for protecting that data, so if the data is on the source side residing on a static disk, then yes, encrypting that data on that disk would be known to people of ordinary skill in the art and, similarly, for data on the destination side.

Kuenning Dep. 7:9–20. Also, in his first declaration, Dr. Kuenning states:

> 51. At the time of the invention, a person of ordinary skill in the art would have understood that data could be secured when it is being stored in files on servers and recognized that encryption techniques could be used to secure it. Such a person would have some understanding of circumstances when it would be desirable to secure this data and also would have understood or perceived that there were potential negative performance impacts of encryption in terms of processing resources for the (en)(de)cryption operations, system response time, and administrative overhead for key management, replication, backup and recovery.
>
> 52. A person of ordinary skill in the field would have known about various disk-based encryption technologies for data in storage (e.g., to protect against theft). A person of ordinary skill in the art furthermore would have understood the security benefits provided by such technologies in the context of a conventional network system. Examples of such known technologies are discussed in the various secondary references cited in the Petition for . . . IPR2014-00245 (Paper 2 or "Petition") and are also discussed in the Declaration of Steven Landauer . . . These references include Stein . . . , Rarick . . . , Anand . . . , and Gleichauf . . . .

Kuenning Decl. ¶¶ 51–52.

Although "'the [obviousness] analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim,'" "'there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007). Also, "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR,* 550 U.S. at 416. Petitioner contends that modifying McCanne "to encrypt data at both the sending and receiving side device would have been a predictable result." Opp. 14.

McCanne describes TAs or WAN optimization devices, a transmitting TA communicating with a receiving TA, providing each TA with its own PSS, and storing encrypted segment data in a PSS of the transmitting TA. Ex. 1003 ¶¶ 48, 61, 87, Table 1, Figs. 1, 2; Kuenning Dep. 8:16–19, 10:12–22. Providing the receiving TA with the encrypting and storing of data performed at the transmitting TA uses elements and methods taught by McCanne. Therefore, we determine that Petitioner's proposed modification combines the elements of McCanne in accordance with its teachings to yield the predictable result of securing data–the well-known function of encryption, which Patent Owner acknowledges (*see* Mot. 12)–stored on both sending and receiving WAN optimization devices, as argued by Petitioner. *See* Opp. 14.

Petitioner also contends that one of ordinary skill in the art would have had reason to modify McCanne so that its receiving TA encrypts received data and stores the encrypted, received data in its PSS because of security concerns for the data stored on WAN optimization devices. *See* Opp. 14. As discussed above, McCanne describes that the bindings table of its PSS stores data with a field that identifies the data encoding method as "encrypted." Ex. 1003 ¶ 87, Table 1. McCanne, thus, suggests or motivates providing security to data stored in its PSS because McCanne describes that the data encoding method can be "encrypted." *See id.* McCanne further describes that the same data may be stored in the PSS's of both transmitting and receiving TAs. *See* Ex. 1003 ¶ 70 ("Because the segments can be uniquely named and the names can be independent of the transaction, a segment appearing in one transaction can be stored at both TAs and used for accelerating other transactions."). Therefore, if security of data stored in the

PSS of a transmitting TA is a concern as suggested by McCanne, then security of the same data stored in the PSS of a receiving TA may also be a concern. Thus, we determine that McCanne suggests or motivates providing security to the same data stored in PSS's of the transmitting and receiving TA.

Petitioner cites a reference in support of its rationale for its proposed modification. *See* Opp. 14 (citing Ex. 1013). Patent Owner argues that the reference is not a printed publication and is not prior art under 35 U.S.C. § 102. *See* Reply 2–4 (discussing Exs. 1012, 1013). A particular prior art reference used to show motivation for a proposed modification, however, is not required as part of an obviousness case. *See KSR,* 550 U.S. at 419. Also, we determine that McCanne itself provides a suggestion or motivation for Petitioner's proposed modification.

Importantly, Patent Owner acknowledges that "[a]t the time of the invention, a person of ordinary skill in the art would have understood that data could be secured using encryption when it is being stored in files and that data could be secured using encryption when being transmitted between servers and clients." Mot. 12 (citing Kuenning Decl. ¶¶ 51–53). Patent Owner argues that an ordinarily skilled artisan "would not have appreciated the data security risks and vulnerabilities posed by WAN optimization devices" and "data security risks in the context of data stored at WAN optimization devices were generally unaddressed prior to the invention of the proposed substitute claims." *Id.* (citing Kuenning Decl. ¶¶ 54–66). Patent Owner cites U.S. Patent No. 8,613,071 to Day (Ex. 2002, "Day")[7],

[7] Patent Owner states that "Day . . . discloses a WAN optimization system that performs encryption at the receiving TA, but does not write this

which Patent Owner does not concede to have a filing date or claimed priority date that is earlier than Patent Owner's date of invention. *Id.* at 12–13 (citing Day, 8:50–9:3, Kuenning Decl. ¶ 55); *see also* Tr. 31:17–33:5 (acknowledging that no evidence or analysis has been presented to verify Patent Owner's position). Patent Owner also argues that "there was little to no recognition by those ordinarily skilled in the field, of data security risks posed by unencrypted data in optimization appliances" and "optimization appliances were not perceived to pose the same risk as databases or other long-term storage." *Id.* at 13 (citing Kuenning Decl. ¶¶ 19, 66).

Although McCanne may not disclose explicitly that security of data stored at WAN optimization devices was a concern, McCanne suggests

encrypted data to the storage of [the] receiving TA" and "the receiving TA encrypts only the outgoing re-assembled data (i.e., the decoded data after all store/retrieve instructions are processed) to the client/server." Mot. 12–13 (citing Day 8:50–9:3, Kuenning Decl. ¶ 55); *see also* Tr. 22:13–25:9 (discussing Day). Patent Owner appears to be relying on Day to demonstrate patentability of the proposed substitute claims, even though Patent Owner contends that Day is not prior art. Nevertheless, to address fully the patentability of the proposed substitute claims, we note that Day discloses encryption of data received at a destination-site appliance. *See* Ex. 2002, col. 8, l. 66–col. 9, l. 3 ("Client-side transaction accelerator 320c de-optimizes the received network traffic and applies the appropriate encryption to the de-optimized network traffic before sending it via secure connection 312b to client 310c."). In response to this particular disclosure, Patent Owner argued at the oral hearing that the proposed substitute claims are distinguishable from Day based on Patent Owner's understanding of Day's description of the type of encryption performed and the purpose of the encryption of data received at a destination-site appliance. Tr. 25:10–31:16. We are not persuaded, however, that Day supports Patent Owner's understanding, as the reference expressly discloses the encryption of received data at the destination-site appliance—the same feature that Patent Owner contends is lacking in McCanne.

encrypting data stored at a WAN optimization device, because it describes that the data segments stored in a PSS of a transmitting TA can be stored with a field that identifies the data encoding method as "encrypted." *See* Ex. 1003 ¶ 87, Table 1. The cited portions of Dr. Kuenning's testimony also do not refer to any support for the assertion that those skilled in the art did not perceive data stored in a WAN optimization device to be at risk, like the data in a database or other long-term storage. Thus, Patent Owner's arguments regarding recognition in the art of a security concern in WAN optimization devices are not persuasive.

Patent Owner also argues that "it was generally thought that encryption and decryption of stored data came with a performance tradeoff that were undesirable and ran counter to the purpose of WAN optimization devices, which are intended to accelerate network transactions." Mot. 13–14 (citing Kuenning Decl. ¶¶ 67–68). A proposed modification may have simultaneous advantages and disadvantages, but that does not necessarily obviate any or all reasons to combine teachings. *See Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000) ("The fact that the motivating benefit comes at the expense of another benefit, . . . should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another. Instead, the benefits, both lost and gained, should be weighed against one another."). Thus, we are not persuaded that a tradeoff between performance and security necessarily obviates a reason to modify McCanne.

Petitioner states, and we agree, that "Patent Owner does not individually argue the patentability of any of the proposed substitute claims other than the above discussed portions of claim 25." Opp. 15; *see also* Mot.

9–15 (arguing allowability of proposed substitute claims), Reply 2–5 (arguing patentability over McCanne). For the foregoing reasons, we determine that Patent Owner has not met its burden of proof to demonstrate patentability of its proposed substitute claim 25, or the other proposed substitute claims, over the prior art. Therefore, we deny Patent Owner's Motion to Amend as to proposed substitute claims 25–48 under 37 C.F.R. § 42.121(a)(2)(i).

5. Proposed Substitute Claims 39–45 and 48

As explained above, Patent Owner bears the burden of proof to show that it is entitled to the relief it requests—namely, entry of the proposed substitute claims. *See supra* Section II.B; 37 C.F.R. § 42.20(c). This requires that Patent Owner make a sufficient showing of patentability over the prior art under 35 U.S.C. §§ 102 and 103, but also that the proposed substitute claims be patent-eligible in the first place. *See Ariosa Diagnostics v. Isis Innovation Ltd.*, Case IPR2012-00022, slip op. at 50–53 (PTAB Sept. 2, 2014) (Paper 166) (denying the patent owner's motion to amend in an *inter partes* review for failure to demonstrate that the proposed substitute claims recited patent-eligible subject matter under 35 U.S.C. § 101); *Volusion, Inc. v. Versata Software, Inc.*, Case CBM2013-00017, slip op. at 4–5 (PTAB Dec. 20, 2013) (Paper 19) (concluding, in a covered business method patent review where the sole ground was eligibility under 35 U.S.C. § 101, that the patent owner was required to demonstrate patentability over the prior art); *id.*, slip op. at 2–5 (PTAB Jan. 27, 2014) (Paper 24). In many cases, particularly where a proposed amendment merely adds limitations to an original patent claim, patent eligibility will be clear. With respect to proposed substitute claims 39–45 and 48, in addition to the reasons discussed above regarding patentability, we are not persuaded that these claims recite patent-eligible subject matter under 35 U.S.C. § 101.

Proposed substitute claim 39 recites:

> 39. A software product for ensuring compliance in network memory comprising:
>
> software operational when executed by a processor to direct the processor to intercept original data sent from a source-site computer to a destination-site computer, encrypt the original data in a source-site appliance to generate encrypted data, store the encrypted data in a first memory device within the source-site appliance, determine whether a representation of the original data exists in a destination-site appliance, transmit a store instruction comprising the original data from the source-site appliance based on the determination that the representation of the original data does not exist in the destination-site appliance, receive the store instruction into the destination-site appliance, encrypt the original data received with the store instruction at the destination-site appliance to generate encrypted received data, store the encrypted received data in a second memory device within the destination-site appliance, subsequently receive a retrieve instruction into the destination-site appliance, the retrieve instruction comprising an index at which the encrypted received data is stored, process the retrieve instruction to obtain encrypted response data in the destination-site appliance, the encrypted response data comprising at least a portion of the encrypted received data, and decrypt the encrypted response data in the destination-site appliance; and
>
> a storage medium that stores the software.

Proposed substitute claims 40–45 and 48, which depend from proposed substitute claim 39, likewise recite a “software product,” and further limit the steps performed by software when executed by a processor and limit the “destination-site computer.” Mot. 6–7.

A claim directed to a transitory, propagating signal is not statutory subject matter under any of the four categories of 35 U.S.C. § 101: "process, machine, manufacture, or composition of matter." *In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007). "If a claim covers material not found in any of the four statutory categories, that claim falls outside the plainly expressed scope of § 101 even if the subject matter is otherwise new and useful." *Id.* at 1354. Terms like "machine-readable storage medium," when given their broadest reasonable interpretation, may encompass a transitory signal, particularly when the specification is silent on the issue. *See Ex parte Mewherter*, No. 2012-007692, 2013 WL 4477509, at *2–7 (PTAB May 8, 2013) (precedential) ("*Mewherter*"); U.S. Patent & Trademark Office, *Subject Matter Eligibility of Computer Readable Media*, 1351 Off. Gaz. US Pat. Off. 212 (Feb. 23, 2010) ("The broadest reasonable interpretation of a claim drawn to a computer [readable] medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent."); *see also Allvoice Developments US, LLC v. Microsoft Corp.*, No. 2014-1258, 2015 WL 2445055, at *8 (Fed. Cir. May 22, 2015) ("instructions, data, or information alone, absent a tangible medium, is not a manufacture").

Proposed substitute claims 39–45 and 48 each recite a "software product" comprising "software," which will be executed by a processor, and a "storage medium that stores the software." Mot. 5–7. The language of the claims themselves does not preclude the storage medium from being a transitory signal. Nor does the Specification of the '684 patent define the terms or limit the claim language to a non-transitory embodiment. Instead, the Specification provides that "software" is simply an example of "executable instructions," and describes examples of "storage media" where such instructions may be stored:

> The above-described functions can be comprised of executable instructions that are stored on storage media. The executable instructions can be retrieved and executed by a processor. Some examples of executable instructions are software, program code, and firmware. Some examples of storage media are memory devices, tape, disks, integrated circuits, and servers. The executable instructions are operational when executed by the processor to direct the processor to operate in accord with the invention. Those skilled in the art are familiar with executable instructions, processor(s), and storage media.
>
> The above description is illustrative and not restrictive. Many variations of the invention will become apparent to those of skill in the art upon review of this disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the appended claims along with their full scope of equivalents.

Ex. 1001, 17:23–39. Applying the broadest reasonable interpretation of claims 39–45 and 48, we interpret the claims as encompassing both transitory and non-transitory media, and as a result, conclude that the claims do not recite patent-eligible subject matter under 35 U.S.C. § 101. The situation is akin to that presented in *Mewherter*, where the claims recited a "machine readable storage medium having stored thereon a computer program, . . . the computer program comprising a routine set of instructions for causing [a] machine to perform" certain steps, and the Specification did not limit the claimed storage medium to being non-transitory. 2013 WL 4477509, at *1.

Patent Owner does not address in its Motion to Amend whether proposed substitute claims 39–45 and 48 recite patent-eligible subject matter under 35 U.S.C. § 101. At the oral hearing, Patent Owner argued that no reasonable interpretation of these claims would read on a purely transitory medium. Tr. 33:6–19. In addition to the fact that Patent Owner's argument was not raised in its papers, we are not persuaded that the Specification limits the claims to solely a non-transitory medium, as it only discloses non-limiting examples of storage media. *See* Ex. 1001, 17:23–39.

Patent Owner's Motion to Amend is denied as to proposed substitute claims 39–45 and 48 because Patent Owner has not shown that the claims recite patent-eligible subject matter under 35 U.S.C. § 101.

III. ORDER

Based on the record presented in this proceeding, Patent Owner has not met its burden with respect to proposed substitute claims 25–48.

In consideration of the foregoing, it is hereby:

ORDERED that Patent Owner's Motion to Amend is *granted* to the extent it requests cancellation of claims 1–24 of the '684 patent;

FURTHER ORDERED that Patent Owner's Motion to Amend is *denied* as to proposed substitute claims 25–48;

FURTHER ORDERED that Exhibit 2015 is expunged from the record in accordance with Paper 36; and

FURTHER ORDERED that, because this is a final written decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirement of 37 C.F.R. § 90.2.

PETITIONER:

David M. O’Dell
Kyle Howard
John Russell Emerson
Andrew S. Ehmke
HAYNES AND BOONE, LLP
david.odell.ipr@haynesboone.com
kyle.howard.ipr@haynesboone.com
russell.emerson.ipr@haynesboone.com
andy.ehmke.ipr@haynesboone.com

PATENT OWNER:

Darren E. Donnelly
Jason Amsel
FENWICK & WEST LLP
ddonnelly-ptab@fenwick.com
jamsel-ptabr@fenwick.com