

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETAPP, INC.,
Petitioner,

v.

KOM SOFTWARE, INC.,
Patent Owner.

IPR2019-00604
Patent 7,536,524 B2

Before KIMBERLY McGRAW, DANIEL J. GALLIGAN, and
BRENT M. DOUGAL, *Administrative Patent Judges*.

GALLIGAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, NetApp, Inc. (“Petitioner”)¹ challenges the patentability of claims 1–4, 9, 11, 18, 19, 24, and 29–31 of U.S. Patent No. 7,536,524 B2 (“the ’524 patent,” Ex. 1001), which is assigned to KOM Software, Inc. (“Patent Owner”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a), addresses issues and arguments raised during the trial in this *inter partes* review. For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–4, 9, 11, 18, 19, 24, and 29–31 of the ’524 patent are unpatentable. *See* 35 U.S.C. § 316(e) (“In an *inter partes* review instituted under this chapter, the petitioner shall have the burden of proving a proposition of unpatentability by a preponderance of the evidence.”).

A. Procedural History

On January 28, 2019, Petitioner requested *inter partes* review of claims 1–4, 9, 11, 18, 19, 24, and 29–31 of the ’524 patent on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	102(e) ²	Vossen ³
1	103(a)	Vossen

¹ Hewlett Packard Enterprise Company (“HPE”) was a petitioner on the original Petition, but this *inter partes* review has since been terminated as to HPE. *See* Paper 23.

² The Leahy-Smith America Invents Act (“AIA”) included revisions to 35 U.S.C. §§ 102 and 103 that became effective after the filing of the application for the ’524 patent. Therefore, we apply the pre-AIA versions of these sections.

³ US 6,026,402, filed Jan. 7, 1998, issued Feb. 15, 2000 (Ex. 1005).

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
2–4, 18, 19	103(a)	Vossen, Denning ⁴
9, 11, 29–31	103(a)	Vossen, Denning, McGovern ⁵
24	103(a)	Vossen, Kung ⁶
1	102(a)	Nagar ⁷
1	103(a)	Nagar
2–4, 18, 19	103(a)	Nagar, Denning
9, 11, 29–31	103(a)	Nagar, Denning, McGovern
24	103(a)	Nagar, Kung

Paper 3 (“Pet.”), 9. Patent Owner filed a Preliminary Response. Paper 9 (“Prelim. Resp.”). We instituted trial on all grounds of unpatentability. Paper 10 (“Dec. on Inst.”), 16.

During the trial, Patent Owner filed a Response (Paper 13, “PO Resp.”), Petitioner filed a Reply (Paper 15, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 25, “PO Sur-reply”).

An oral hearing was held on May 27, 2020, a transcript of which appears in the record. Paper 32 (“Tr.”).

B. Related Matters

As required by 37 C.F.R. § 42.8(b)(2), the parties identify various related matters. Pet. 76–77; Paper 4, 2–3; Paper 8, 2–3; Paper 27, 1–2.

⁴ Dorothy Elizabeth Robling Denning, *Cryptography and Data Security* © 1982 (“Denning”) (Ex. 1006).

⁵ US 2005/0097260 A1, filed Nov. 3, 2003, published May 5, 2005 (Ex. 1007).

⁶ US 5,265,159, issued Nov. 23, 1993 (Ex. 1008).

⁷ Rajeev Nagar, *Windows NT File System Internals: A Developer’s Guide* © 1997 (“Nagar”) (Ex. 1009).

C. Real Parties in Interest

The parties identify themselves as the real parties in interest. Pet. 76; Paper 4, 2; Paper 8, 2; Paper 27, 1.

D. The '524 Patent and Illustrative Claim

The '524 patent generally relates to providing access privileges for a computer storage medium. Ex. 1001, 2:35–38. The '524 patent explains that an attempted operation is intercepted and compared to the operation access privileges associated with a storage medium to determine whether to allow or deny the attempted operation. Ex. 1001, 3:64–4:8. The '524 patent identifies read and write, among others, as examples of operation access privileges. Ex. 1001, 4:50–54.

Of the challenged claims, claims 1 and 29 are independent. Claim 1 is illustrative and is reproduced below.

1. A method for applying an operation access privilege to a storage medium, comprising:
 - associating an access privilege with at least a portion of the storage medium;
 - intercepting an attempted operation on said at least a portion of the storage medium, wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation;
 - comparing the attempted operation to the access privilege;
 - and
 - allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege.

II. ANALYSIS

A. Level of Ordinary Skill in the Art

Petitioner contends a person of ordinary skill at the time of the invention of the '524 patent (a “POSITA”) “would have held either a

bachelor's degree in computer engineering or computer science with two years of experience in the field of data storage management or a master's degree in either discipline with an emphasis on data storage management." Pet. 9 (citing Ex. 1002 ¶¶ 46–50). Patent Owner provides a similar definition, stating "a POSITA should have a bachelor's degree in electrical engineering, computer science, or equivalent with two years or more of experience in computing systems development; a master's degree in electrical engineering, computer science, or equivalent; or comparable computing systems work experience." PO Resp. 14 (citing Ex. 2001 ¶ 38).

Thus, the parties dispute whether a POSITA must have a degree in computer science/engineering or whether a POSITA could instead have a degree in electrical engineering as well as whether the POSITA's experience must be in data storage management or could encompass experience in the field of computing systems development. *See* Ex. 2001 ¶ 32 (Dr. Melendez testifying that a POSITA may also have a degree in electronics engineering or applied mathematics).

Although the parties articulate different levels of skill for a POSITA, neither party explains how its recited level of skill impacts the obviousness analysis such that application of one proposal versus the other would lead to different ultimate outcomes.

Based on the record before us, including the types of problems and solutions described in the '524 patent and the cited prior art, we determine that a person of ordinary skill in the art would have had a bachelor's degree in a technical field such as computer engineering, computer science, electrical engineering, electronics engineering, applied mathematics, or their equivalent, with two years of experience in the field of computing systems

development, including fields of data storage management or file storage and manipulation; a master's degree in such a technical field; or comparable computing systems work experience. We further note that our analysis would be the same under either parties' definition.

B. Claim Interpretation

The Petition was accorded a filing date of January 28, 2019. Paper 6, 1. In an *inter partes* review for a petition filed on or after November 13, 2018, a claim “shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). In applying this claim construction standard, we are guided by the principle that the words of a claim “are generally given their ordinary and customary meaning,” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc) (citation omitted). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). There is a “heavy presumption” that a claim term carries its ordinary and customary meaning. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) (citation omitted).

1. Associating

Although both parties assert that none of the claim terms needs to be construed expressly (Pet. 10; PO Resp. 14–15), the parties dispute the meaning of the phrase “associating an access privilege with at least a portion of the storage medium,” as recited in claims 1 and 29. Patent Owner argues that a person of ordinary skill in the art “understands that ‘associating an access privilege with at least a portion of the storage medium’ means to combine or join the operation access privileges within at least a portion of the storage medium.” PO Resp. 23 (citing Ex. 2001 ¶ 53); *see also* PO Resp. 27 (stating “the inventive steps taught within the ’524 Patent” require that “the storage medium itself maintains its associated operation access privileges independent of the computer” (citing Ex. 1001, 11:57–12:7, Fig. 6; Ex. 2001 ¶ 60)); PO Sur-reply 12–17. During oral argument, Patent Owner clarified that the claimed “associating” language requires that the access privilege be “stored in the storage medium.” Tr. 59:12–60:10; *see also* Tr. 60:19–20 (stating that “[i]t has to be stored in whatever storage medium is being mounted”). Petitioner argues that construing the “associating” phrase as Patent Owner proposes would improperly import an unclaimed embodiment from the Specification into the claims. Pet. Reply 14. For the reasons explained below, we agree with Petitioner.

We begin our analysis with the claim language. *In re Power Integrations, Inc.*, 884 F.3d 1370, 1376 (Fed. Cir. 2018) (“Claim construction must begin with the words of the claims themselves.” (brackets and citation omitted)). The disputed phrase recites “associating an access privilege with at least a portion of the storage medium.” The independent claims do not recite “combine,” “join,” or “store” as proposed by Patent

Owner. Neither “combine” nor “join” appear anywhere in the ’524 patent. Nor does the ’524 patent state that the access privilege *must* be stored in the storage medium. *See, e.g.*, Ex. 1001, 11:57–12:7, Fig. 6 (describing a preferred embodiment). It makes some sense to consider data stored in a storage medium to be associated with that storage medium simply by virtue of being stored there. But the converse—that associating with a storage medium requires storing in the storage medium—does not follow from a plain and ordinary reading of the claim language. The record does not contain persuasive evidence or argument showing that the plain and ordinary meaning of “associating” means “storing.” Therefore, we turn to the Specification, which “is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.” *Phillips*, 415 F.3d at 1315 (internal quotation and citation omitted).

Patent Owner’s argument rests largely on the disclosure of the ’524 patent pertaining to Figure 6, which is reproduced below. *See* PO Resp. 23–24 (discussion of Figure 6); PO Sur-reply 13–14.

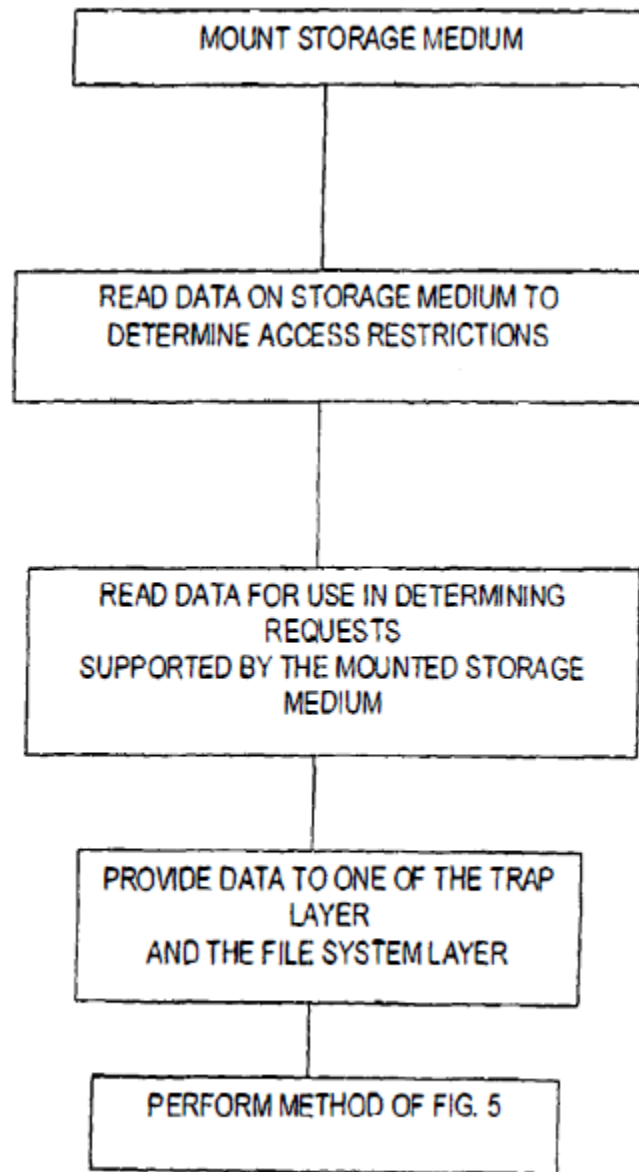


FIG. 6

Figure 6 of the '524 patent, reproduced above, is “a simplified flow diagram of a method of providing software settable access privileges within Windows NT® is shown.” Ex. 1001, 11:57–59. Referring to Figure 6, the '524 patent explains the following:

A storage medium is mounted within a computer system. The storage medium has stored thereon data relating to access

privileges for the storage medium. Upon mounting the storage medium, data relating to physical limitations of the read/write device are loaded into the device driver for that device within the file system layer. The limitations are recognised by the system software. Also upon mounting the storage medium, the data relating to access privileges for the storage medium are loaded into the trap layer.

Ex. 1001, 11:59–12:1.

Citing the '524 patent's disclosure pertaining to Figure 6, Patent Owner argues that “the '524 Patent teaches that the operation access privileges are associated with the mounted storage medium and not with the computer's programs and executing processes.” PO Resp. 24 (citing Ex. 1001, Fig. 6; Ex. 2001 ¶ 54). Patent Owner asserts that “the storage medium itself maintains its associated operation access privileges independent of the computer.” PO Resp. 27 (citing Ex. 1001, 11:57–12:7, Fig. 6; Ex. 2001 ¶ 60).

Although the method of Figure 6 clearly involves reading access privilege data that are stored on the storage medium (Ex. 1001, 11:60–12:1), claims 1 and 29 do not recite “reading access privilege data from the storage medium” any more than they recite “storing access privilege data on the storage medium.” Patent Owner's proposed construction in effect would rewrite the claim to require reading the privileges from the storage medium. Patent Owner stated as much during oral argument: “[I]t's our position that the associating step is when you perform the method and the only method of getting these operation access privileges off of the storage medium, such that, you know, that the invention can actually be accomplished is through this methodology.” Tr. 57:2–8.

In the particular embodiment of Figure 6, it can be assumed that the access privileges are associated with the storage medium by being stored there, but the '524 patent's description of Figure 6 does not show that associating privileges with a storage medium can only be accomplished by storing them on the storage medium. The claims recite "associating," and the Specification of the '524 patent does not equate "associating" and "storing."

Indeed, other claims of the '524 patent use the word "storing." *See, e.g.,* Ex. 1001, claims 6 ("6. The method according to claim 2, wherein said enforcing comprises storing said at least one policy with at least one of: an alternate data stream, an extended attribute, or a private data."), 25 ("25. The method according to claim 1, further comprising obfuscating user data by storing said user data in at least one of: an alternate data stream or an alternate location."). The applicant's use of "associating" as opposed to "storing" in claim 1, absent some lexicography equating the two terms, indicates that Patent Owner understood the two terms to have different meanings and that claims 1 and 29 are not as limited as Patent Owner proposes.

In addition to Figure 6 from the '524 patent, Patent Owner cites the Abstract and column 3, lines 22–33 in its discussion of the "associating" limitation, but Patent Owner provides no substantive discussion of these passages to show how they support a construction of "associating" to mean "storing." *See* PO Resp. 23. The Abstract of the '524 patent discloses "restricting file access . . . wherein a set of file write access commands are determined from data stored within a storage medium." Ex. 1001, code (57). The Abstract, however, does not mention "associating" or "access

privilege,” and Patent Owner provides no persuasive explanation how this disclosure in the Abstract limits the claimed “associating” to “storing.” The passage from column 3, lines 22–33 of the ’524 patent is directed to a method involving “providing an indication of a data write access privilege for the entire logical storage medium,” but the passage does not mention “associating,” nor does it say that the access privilege is stored on the storage medium. Ex. 1001, 3:22–33. Thus, we do not view these disclosures from the ’524 patent as supporting Patent Owner’s attempt to limit the claimed “associating” to “storing.”

Patent Owner also cites Figure 5 of the ’524 patent (PO Resp. 23; PO Sur-reply 14), which is “a flow diagram of a method of storing data in a storage medium” and describes that “[t]he trap layer intercepts [a] request [to store data] and the data and determines whether the storage medium selected supports the operation” (Ex. 1001, 11:37–39, 11:45–47). Patent Owner argues that Figure 5 of the ’524 patent “shows how the comparing and allowing/denying steps include logic asking whether *the storage medium itself* supports the operation at issue (such decision reflecting the *data from the storage medium itself* shown in Fig. 6).” PO Sur-reply 14 (citing Ex. 1001, 11:41–47). Patent Owner’s argument based on Figure 5, therefore, rests on its arguments for Figure 6, which we address above. The description of Figure 5 does not mention “associating,” let alone limit associating to “storing.” Thus, we do not view Figure 5 as any more supportive of Patent Owner’s position than Figure 6.

For these reasons, we do not agree with Patent Owner’s proposed interpretation of “associating an access privilege with at least a portion of the storage medium.” No further construction of this phrase or any other

claim term is necessary. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. Principles of Law

To establish anticipation, each and every element in a claim, arranged as recited in the claim, must be found in a single prior art reference. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1371 (Fed. Cir. 2008). Although the elements must be arranged or combined in the same way as in the claim, “the reference need not satisfy an *ipsissimis verbis* test,” i.e., identity of terminology is not required. *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009) (citing *In re Bond*, 910 F.2d 831, 832–33 (Fed. Cir. 1990)).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) any secondary considerations, if in evidence.⁸ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

⁸ Patent Owner does not present any objective evidence of nonobviousness (i.e., secondary considerations) as to any of the challenged claims.

*D. Anticipation by Nagar
(Claim 1)*

Petitioner asserts that claim 1 of the '524 patent is unpatentable under 35 U.S.C. § 102(a) as anticipated by Nagar. Pet. 8–9, 56–64.

1. Nagar

Nagar is a developer's guide for the Windows NT operating system. Ex. 1009. Petitioner argues that Nagar was published in 1997, and therefore qualifies as prior art under 35 U.S.C. § 102(a). Pet. 8 (citing Ex. 1014; Ex. 1015 ¶¶ 6–19; Exs. 1016, 1021–1023). Patent Owner does not challenge the prior art status of Nagar. *See generally* PO Resp. We are persuaded that Petitioner has shown that Nagar qualifies as prior art under 35 U.S.C. § 102(a). *See* Exs. 1014–1016.

Nagar “focuses on file system driver and filter driver implementation for the Windows NT platform” and explains the following:

A filter driver is an intermediate driver that intercepts requests targeted to some existing software module (e.g., the file system or a disk driver). By intercepting the request before it reaches its intended target, the filter driver has the opportunity to either extend, or simply replace, the functionality provided by the original recipient of the request.

Ex. 1009, 12, 51.⁹ Nagar discloses a filter driver that acts as virus detection software by intercepting input/output (I/O) requests and determining whether to allow the operations. Ex. 1009, 52–53, 498–499.

2. Independent Claim 1

Petitioner argues that Nagar's disclosure of a virus-detecting filter driver that layers itself above a logical storage volume and allows or denies access to the logical storage volume based on the type of attempted

⁹ We refer to the exhibit page numbers assigned by Petitioner in Nagar.

operation describes “applying an operation access privilege to a storage medium” and “associating an access privilege with at least a portion of the storage medium.” Pet. 58–60 (citing Ex. 1009, 159, 498–499, 506; Ex. 1002 ¶¶ 183–191). Petitioner argues that Nagar’s disclosure of intercepting all I/O requests to the logical volume describes the “intercepting” step of claim 1. Pet. 60–62 (citing Ex. 1009, 18, 51, 134, 191, 195, 496–499; Ex. 1002 ¶¶ 192–198). Petitioner argues Nagar describes the “comparing” and “allowing, or denying” steps of claim 1 by disclosing that the filter driver checks to see if the request is a read or write request, allows the operation in the case of a read, checks for viruses in the case of a write, allows the write if no virus is detected, and rejects the write if a virus is detected. Pet. 62–64 (citing Ex. 1009, 498–499; Ex. 1002 ¶¶ 199–204).

Petitioner provides the annotated version of Nagar’s Figure 12-2 reproduced below.

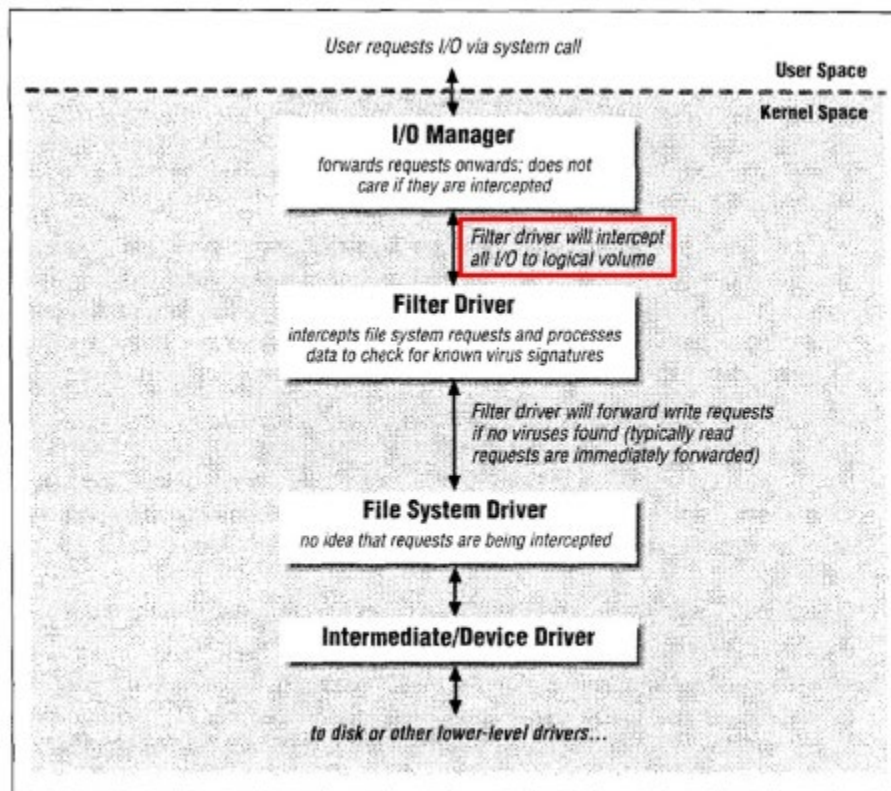


Figure 12-2. Filter driver used in virus detection

Pet. 61. The above annotated version of Figure 12-2 “illustrates how a filter driver that layers itself above a mounted logical volume device object managed by a file system driver can perform the virus detection functionality.” Ex. 1009, 498. Petitioner includes a red box around the text “Filter driver will intercept all I/O to logical volume.” Pet. 61.

Patent Owner argues that Nagar does not describe (a) “applying an operation access privilege”¹⁰ (PO Resp. 27–30) or (b) “associating an access privilege with at least a portion of the storage medium” (PO Resp. 30–34).

¹⁰ This language appears in the preamble of claim 1. We need not decide whether the preambles of the challenged claims are limiting because we find that Petitioner has shown that the preamble recitations are taught by the cited art.

a) Operation access privilege

The preamble of claim 1 requires “applying an operation access privilege to a storage medium.” As noted above and below, various aspects of the claim deal with the access privilege, and, therefore, our discussion in this section also addresses the steps of claim 1 reciting “intercepting an attempted operation on said at least a portion of the storage medium, wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation,” “comparing the attempted operation to the access privilege,” and “allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege.”

Patent Owner argues that Nagar does not teach the claimed operation access privilege because Nagar’s access privileges are based on the content of data (content-based access privileges) to be written to the storage medium, such as whether the data contain viruses, and not based on the attempted operation (operation-based access privileges). PO Resp. 27–30. According to Patent Owner,

[a]n “operation access privilege” as recited in the ‘524 Patent means that the “access privilege” is of the “operation” and not a privilege of executing processes associated with application programs running within a computer or the determination of the purity of data [i.e. content] to be written as in Nagar.”

PO Resp. 27 (citing Ex. 2003, 43; Ex. 1009, 498–499; Ex. 2001 ¶ 62).

We disagree with Patent Owner’s attempted distinction over Nagar. The ’524 patent lists exemplary “operation access privileges” as follows: “read, write, execute, move, rename, append, change permissions, change attributes, overwrite and/or overwrite zero length.” Ex. 1001, 4:50–54. Petitioner is correct in asserting that Nagar discloses “differentiat[ing]

between types of access operations acting on logical volumes (e.g., read and write requests).” Pet. 58 (citing Ex. 1009, 498–499). Nagar discloses that

the filter driver module intercepts the I/O before it reaches the file system. Now, the virus-detection module can check for any virus signatures in the data being written out to disk. Note that in most cases, read requests can be immediately forwarded by the filter driver to the file system.

Ex. 1009, 499. Thus, Nagar expressly discloses two operation access privileges identified in the ’524 patent—read and write. Ex. 1009, 498–499.

In the case of a read, Nagar discloses allowing (forwarding) the operation because it is a read request. Ex. 1009, 499; *see* Ex. 1002 ¶ 204 (Dr. Weissman testifying that a person of ordinary skill in the art would have understood forwarding to mean “allowing” as recited in the claim). Patent Owner acknowledges this in arguing that, “[e]ven when Nagar only forwards read requests, these are privileges applied to read requests and not privileges applied to a storage medium.” PO Resp. 28 n.2 (citing Ex. 1009, 498–499; Ex. 2001 ¶ 62 (testifying similarly)). Thus, Nagar discloses comparing the attempted operation to the access privilege and allowing read requests based on the fact that they are read requests, satisfying even Patent Owner’s asserted requirement that the access privilege must be dependent “solely upon the operation itself” (operation-based as opposed to content-based). *See* PO Resp. 28. Claim 1 recites “allowing, or denying,” and, therefore, Nagar’s disclosure for the read operation alone is sufficient to meet this step. We find that Nagar’s disclosures of determining whether a request is a read request or a write request and forwarding read requests describe “comparing the attempted operation to the access privilege” and “allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege.”

Furthermore, we do not agree that claim 1's operation must be based *solely* on the attempted operation and cannot also take other things into account, such as content of data, as Patent Owner asserts. *See* PO Resp. 28. To support this argument, Patent Owner cites to, *inter alia*, the prosecution history of U.S. Patent No. 7,076,624 ("the '624 patent"), which is related to the '524 patent. *See* PO Resp. 28 (citing Ex. 2003 (Prosecution History of U.S. Patent No. 7,076,624), 43). The cited statements of the '624 patent's prosecution history, however, were directed to the language of the pending claims in that application reciting that intercepting an attempted operation "occurs regardless of an identity of a user." *See* Ex. 2003, 34, 36, 39, 43. This claim language does not distinguish over Nagar, which describes precisely this subject matter. In particular, claim 1 of the '524 patent similarly recites "intercepting an attempted operation on said at least a portion of the storage medium, wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation." Nagar discloses that its "[f]ilter driver will intercept all I/O to logical volume." Ex. 1009, 498 (Fig. 12-2), *reproduced at* Pet. 58. During the trial, Patent Owner did not dispute that Nagar's disclosure of intercepting all input/output requests describes this subject matter. *See generally* PO Resp. 27–34.¹¹ Because Nagar discloses intercepting all operations, we find that it describes

¹¹ Before institution, Patent Owner argued that Nagar does not describe the "intercepting" step of claim 1. Prelim. Resp. 11–13. In our Institution Decision, we addressed this argument, citing Nagar's disclosure of intercepting all input/output requests. Dec. on Inst. 14. Patent Owner did not contest the issue during trial and, therefore, waived any arguments for this limitation. *See* Paper 11, 7 ("Patent Owner is cautioned that any arguments not raised in the response may be deemed waived.").

intercepting an attempted operation “regardless of an identity of a user,” as recited in claim 1.

Contrary to Patent Owner’s argument based on the prosecution history of the ’624 patent, claim 1 does not prohibit other considerations in determining whether to allow or deny an attempted operation. Rather, claim 1 requires “allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege.” Nagar discloses rejecting a write request if a virus is detected and forwarding (allowing) the write request if no virus is detected. Ex. 1009, 499, *cited in* Pet. 59. We find, therefore, that Nagar describes allowing or denying the write request based on comparing the attempted operation to the access privilege, even if Nagar bases the decision on other factors as well, such as the presence of a virus.

Based on the foregoing discussion and Petitioner’s persuasive contentions, we find Nagar describes “[a] method for applying an operation access privilege to a storage medium.” For reasons discussed above, we also find Nagar describes the steps of claim 1 reciting “intercepting an attempted operation on said at least a portion of the storage medium, wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation,” “comparing the attempted operation to the access privilege,” and “allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege.”

*b) Associating an access privilege with at least
a portion of the storage medium*

Patent Owner argues that “associating an access privilege with at least a portion of the storage medium,” as required by claim 1, means that “the

storage medium itself maintains its associated operation access privileges— independent of the computer.” PO Resp. 31–32. As discussed above in § II.B.1, we do not agree that the claimed “associating” requires that the storage medium store the access privileges.

We are persuaded that Nagar describes the claimed “associating.” *See* Pet. 59–60 (citing Ex. 1009, 159, 498–499, 506; Ex. 1002 ¶¶ 189–191). In particular, Nagar discloses that “a filter driver that layers itself above a mounted logical volume device object managed by a file system driver can perform the virus detection functionality.” Ex. 1009, 498. Nagar also explains that filter drivers “intercept I/O requests targeted to certain device objects by interjecting themselves into the driver hierarchy and by *attaching themselves to the target device objects*.” Ex. 1009, 159 (emphasis added).

Patent Owner argues that Petitioner’s reliance on a *logical* storage medium in Nagar fails because the claim recites a “storage medium.” PO Sur-reply 8. The ’524 patent, however, states that, “[a]ccording to an exemplary aspect of the present invention, the method may include wherein the storage medium is a logical storage medium.” Ex. 1001, 4:13–15. Thus, the Specification of the ’524 patent shows that a logical storage medium is considered a storage medium, and the claims do not prohibit the use of a logical storage medium. Thus, we disagree with Patent Owner’s argument that Petitioner’s reliance on a logical storage medium in the prior art fails to show a storage medium. *See* PO Sur-reply 8.

Patent Owner also argues that Petitioner’s reliance on Nagar’s disclosure of attaching a filter driver to a device object fails because “the device object is only a representation of a mounted logical volume and not the actual storage medium itself” and because a person of ordinary skill in

the art “would not understand a representation of a mounted logical volume to be the same as the actual portion of a storage medium.” PO Resp. 32 n.3 (citing Ex. 1009, 499; Ex. 2001 ¶ 68). Patent Owner’s argument and Dr. Melendez’s testimony, however, ignore Nagar’s disclosure of what a device object is. *See* Pet. Reply 16–17 (citing Ex. 1009, 155–156, 279, 285–286, 506; Ex. 1002 ¶¶ 206–208). Nagar explains that “[d]evice object structures are created by kernel-mode drivers to represent logical, virtual, or physical devices. For example, a physical device, such as a disk drive, is represented in memory by a device object.” Ex. 1009, 155–156. Nagar further explains that, “if you develop a disk driver and do not create a device object structure representing this particular disk device, no user process can access this disk.” Ex. 1009, 156. Thus, we agree with Petitioner’s assertion that “associating with a storage medium is achieved by attaching to a device object, because a computer views the storage medium as a device object.” *See* Pet. Reply 16–17 (citing Ex. 1009, 155–156, 506).

In its Sur-reply, Patent Owner argues that Nagar does not disclose that access privileges are stored in the storage medium. PO Sur-reply 16–17. As discussed above § II.B.1, we do not agree with Patent Owner’s contention that the claimed “associating” requires that the access privileges be stored in the storage medium.

Based on the foregoing discussion and Petitioner’s persuasive contentions, we find Nagar describes “associating an access privilege with at least a portion of the storage medium.”

c) Determination of unpatentability

For the reasons discussed above, we find that Nagar describes the subject matter recited in claim 1, and, therefore, Petitioner has proven by a

preponderance of the evidence that claim 1 of the '524 patent is unpatentable under 35 U.S.C. § 102(a) as anticipated by Nagar.

*E. Obviousness over Nagar
(Claim 1)*

Petitioner also asserts that claim 1 of the '524 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over the teachings of Nagar. Pet. 8–9, 64–68. “[I]t is well settled that ‘a disclosure that anticipates under § 102 also renders the claim invalid under § 103, for ‘anticipation is the epitome of obviousness.’” *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1373 (Fed. Cir. 2019) (quoting *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983)). Because we find Nagar anticipated claim 1, we also conclude that the subject matter of claim 1 would have been obvious under 35 U.S.C. § 103(a) based on the teachings of Nagar.

*F. Anticipation by Vossen
(Claim 1)*

Petitioner asserts that claim 1 of the '524 patent is unpatentable under 35 U.S.C. § 102(e) as anticipated by Vossen. Pet. 9, 11–19.

1. Vossen

Vossen discloses “restricting a process or process hierarchy to a subset of a computer host’s file system(s) in an environment where all file systems are simultaneously available to an application.” Ex. 1005, 2:3–6.

2. Independent Claim 1

Petitioner contends Vossen’s disclosure of restricting access to certain file system hierarchies describes “applying an operation access privilege to a storage medium” and “associating an access privilege with at least a portion of the storage medium.” Pet. 12–15 (citing Ex. 1005, 1:25–41, 1:49–62, 2:3–23, 2:65–3:5, 3:33–40, 3:59–4:16, 6:7–31, 8:19–49, 9:1–43, 10:5–40,

Fig. 4; Ex. 1002 ¶¶ 76–81). In particular, Petitioner asserts “*Vossen* maintains data structures regulating a process’s rights to access file system hierarchies.” Pet. 14. Petitioner contends that, because “[e]ach file system exists as part of a partition on a hard disk,” *Vossen*’s file system access privileges “pertain to ‘*at least a portion of the storage medium*,’” as recited in claim 1. Pet. 14 (citing Ex. 1003 ¶ 80). Petitioner also contends that “*Vossen*’s restrictions disclose the claimed ‘*operation access privilege*’ because they relate to enabling and restricting operation access to a file, including reading, writing, opening, and creating operations.” Pet. 13 (citing Ex. 1002 ¶ 77; Ex. 1005, 3:59–4:16, 10:29–40; Ex. 1001, 1:26–37).

Petitioner contends *Vossen*’s disclosure that a filter driver receives and examines all Input/Output (I/O) Request Packets (IRPs) that are directed to the file system driver describes the “intercepting” step of claim 1. Pet. 15–17 (citing Ex. 1005, 3:59–4:16, 4:23–30, 4:43–67, 6:1–5, 6:54–57, 7:28–31, 8:25–49, 9:55–10:40, 11:1–12, Fig. 6; Ex. 1002 ¶¶ 82–86). Petitioner argues *Vossen* describes the “comparing” and “allowing, or denying” steps of claim 1 by its disclosure of determining whether there are any file system restrictions for each IRP. Pet. 17–19 (citing Ex. 1005, 4:61–64; 8:19–24, 8:34–49, 9:55–58, 10:5–28, 11:1–4, 11:24–28, Fig. 4; Ex. 1002 ¶¶ 87–92).

Patent Owner argues that *Vossen* does not describe “applying an operation access privilege” (PO Resp. 17–21) or “associating an access privilege with at least a portion of the storage medium” (PO Resp. 21–27).

Patent Owner argues that *Vossen* does not describe an “operation access privilege,” as recited in the preamble of claim 1, because *Vossen* discloses restrictions that “are *user-centric and process-centric*.” PO

Resp. 19. As with its arguments against Nagar, Patent Owner cites the prosecution history of a different patent to argue that “Vossen’s security descriptors necessarily depend on which users are given permission and are not ‘based solely on the operation, and regardless of the user.’” PO Resp. 18 (quoting Ex. 2003, 43) (citing Ex. 2001 ¶ 43). As discussed above in § II.D.2.a, however, this argument was directed to language of the pending claims in that application reciting that intercepting an attempted operation “occurs regardless of an identity of a user.” Ex. 2003, 34, 36, 39.

Similar language appears in the intercepting step of claim 1 of the ’524 patent. Vossen discloses that, “[o]nce the process restriction file system filter is installed, it receives all I/O requests destined for physical file systems.” Ex. 1005, 9:55–56, *quoted in* Pet. 17. Vossen also discloses that, “[f]or each IRP received, the filter driver determines if the process that initiated the I/O request should be subject to file system restrictions.” Ex. 1005, 10:6–8, *cited in* Pet. 17. Because Vossen discloses intercepting all I/O requests, it describes intercepting an attempted operation “regardless of an identity of a user,” as recited in claim 1.

Contrary to Patent Owner’s arguments, claim 1 does not prohibit restrictions that are user-specific or process-specific. Rather, claim 1 recites “applying an operation access privilege to a storage medium” and “associating an access privilege with at least a portion of the storage medium.”

Patent Owner argues that “a ‘process’ in Vossen is not an ‘operation’ as in the ‘524 Patent” and, therefore, that Petitioner’s reliance on Vossen’s disclosure of restricting processes does not describe the claimed subject matter. PO Resp. 20 (citing Ex. 2001 ¶ 46; Ex. 1005, 3:16–19). But as

Petitioner correctly asserts, Vossen’s restrictions relate to particular operations. *See* Pet. 13 (citing Ex. 1002 ¶ 77; Ex. 1005, 3:59–4:16, 10:29–40; Ex. 1001, 1:26–37). For example, Vossen discloses that “[t]he security descriptor contains attributes describing which users or pseudo-users are permitted to access the file, *and in what ways (obtain file contents, modify contents, or both).*” Ex. 1005, 4:1–4 (emphasis added).

We are persuaded by Petitioner’s contention that “*Vossen’s* restrictions disclose the claimed ‘*operation access privilege*’ because they relate to enabling and restricting operation access to a file, including reading, writing, opening, and creating operations.” *See* Pet. 13 (citing Ex. 1002 ¶ 77; Ex. 1005, 3:59–4:16, 10:29–40; Ex. 1001, 1:26–37). As discussed above in § II.D.2.a, the ’524 patent lists exemplary “operation access privileges” as follows: “read, write, execute, move, rename, append, change permissions, change attributes, overwrite and/or overwrite zero length.” Ex. 1001, 4:50–54. Vossen discloses restrictions for operations such as “obtain file contents,” i.e., read, and “modify file contents,” i.e., write. Ex. 1005, 4:1–4; *see* Ex. 1002 ¶ 77 (Dr. Weissman testifying that Vossen’s restrictions “relate to enabling (or restricting) access to a subhierarchy, including reading, writing, opening, and creating access”). Thus, we find Vossen expressly describes two operation access privileges identified in the ’524 patent—read and write.

We also are persuaded, and we find, that Vossen’s restrictions are applied to, and associated with, a storage medium. As discussed above in § II.B.1, we do not agree with Patent Owner’s assertions that “‘associating an access privilege with at least a portion of the storage medium’ means to combine or join the operation access privileges within at least a portion of

the storage medium” or that it means storing the privileges within the storage medium. *See* PO Resp. 23. Vossen discloses “restricting a process or process hierarchy to a subset of a computer host’s file system(s)” by using a SetProcessRootDirectories() function call to “provide[] the path name of a file system hierarchy within which the calling process should be restricted for one or more file systems.” Ex. 1005, 2:3–6, 8:25–31; *see* Pet. 14–15. Vossen also discloses that every hard disk has a certain number of partitions and that “[e]ach partition has the potential to contain a file system.” Ex. 1005, 6:22–25. Because each file system to which restrictions are applied exists on a portion of a storage medium, namely a hard disk partition, we are persuaded, and we find, that Vossen’s disclosure of restricting access to a file system describes “applying” the restriction to, and “associating” the restriction with, a storage medium, as asserted by Petitioner. *See* Pet. 12–15.

Our findings in this regard are consistent with Patent Owner’s characterization of Vossen’s disclosure as follows:

Vossen limits the ability of executing processes associated with application programs and running within a computer from accessing portions of storage that the processes are not authorized to access which a POSITA understands as being manifested in the allowance of access by executing processes to *only certain portions of a logical storage medium*.

PO Resp. 18 (emphasis added) (citing Ex. 1005, code (57), 1:5–8, 1:11–14, 1:63–67, 2:3–6, 2:65–3:1; Ex. 2001 ¶ 44). Thus, even under Patent Owner’s understanding, Vossen describes applying restrictions to a storage medium, even if those restrictions further specify user and process restrictions. That Vossen’s restrictions may further be limited to particular users or processes

does not negate Vossen’s disclosure that the restrictions are associated with the storage medium.

For the “intercepting” step, as discussed above, Vossen discloses that, “[o]nce the process restriction file system filter is installed, it receives all I/O requests destined for physical file systems.” Ex. 1005, 9:55–56, *quoted in* Pet. 17. Thus, because Vossen discloses that all IRPs are intercepted, we find that Vossen describes intercepting an attempted operation on a portion of the storage medium regardless of the identity of the user attempting the operation.

For the “comparing” step, Petitioner argues that Vossen discloses “compar[ing] the IRP to ‘each entry’ in a data structure to determine whether access restrictions apply.” Pet. 17–18 (citing Ex. 1005, 8:34–49, 10:5–28). For the “allowing, or denying” step, Petitioner argues that “the filter driver allows an attempted operation if it finds a match between the requested operation on the file system and an entry in the restriction data structure” and denies the operation if there is no corresponding entry in the restriction data structure. Pet. 19 (citing Ex. 1005, 8:44–49, 10:5–28, 11:1–4, 11:24–28, Fig. 4; Ex. 1002 ¶¶ 90–92).

As with its arguments against Nagar, Patent Owner argues that claim 1’s operation must be based *solely* on the attempted operation: “Vossen’s security descriptors necessarily depend on which users are given permission and are not ‘based solely on the operation.’” PO Resp. 18 (quoting Ex. 2003, 43) (citing Ex. 2001 ¶ 43). As discussed above, however, claim 1 does not require that allowing or denying the operation be based “solely on the operation,” as Patent Owner asserts. Rather, claim 1 requires allowance or denial to be “based on comparing the attempted

operation to the access privilege.” We are persuaded by Petitioner’s contentions, and we find, that allowing or denying access based on “what ways” a user is permitted to access a file, such as “obtain file contents,” i.e., read, or “modify contents,” i.e., write, describes “comparing the attempted operation to the access privilege” and “allowing, or denying the attempted operation based on comparing the attempted operation to the access privilege,” as recited in claim 1.

For the reasons discussed above, we find that Vossen describes the subject matter recited in claim 1, and, therefore, Petitioner has proven by a preponderance of the evidence that claim 1 of the ’524 patent is unpatentable under 35 U.S.C. § 102(e) as anticipated by Vossen.

*G. Obviousness over Vossen
(Claim 1)*

Petitioner also asserts that claim 1 of the ’524 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over the teachings of Vossen. Pet. 9, 19–24. Because we find Vossen anticipated claim 1, we also conclude that the subject matter of claim 1 would have been obvious under 35 U.S.C. § 103(a) based on the teachings of Vossen. *See Realtime Data*, 912 F.3d at 1373.

*H. Obviousness over the Combinations of Vossen and Denning
and Nagar and Denning
(Claims 2–4, 18, 19)*

Petitioner asserts that claims 2–4, 18, and 19 of the ’524 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen and Denning and the combined teachings of Nagar and Denning. Pet. 7–9, 24–38 (discussion of Vossen and Denning), 68–70 (discussion of Nagar and Denning).

1. Denning

Denning is a book titled *Cryptography and Data Security*. Ex. 1006. Petitioner argues that Denning was published in 1982, and therefore qualifies as prior art under 35 U.S.C. § 102(b). Pet. 7–8 (citing Ex. 1017; Ex. 1015 ¶¶ 6–13, 20–24). Patent Owner does not challenge the prior art status of Denning. *See generally* PO Resp. We are persuaded that Petitioner has shown Denning qualifies as prior art under 35 U.S.C. § 102(b). *See* Ex. 1015 ¶¶ 20–24; Ex. 1017.

Denning discloses access controls that ensure authorized access to data. Ex. 1006, 191. Denning discloses that “[a]n access control policy specifies the authorized accesses of a system” and that “an access control mechanism implements or enforces the policy.” Ex. 1006, 191 (emphases omitted).

2. Claims 2–4, 18

Petitioner presents persuasive arguments and evidence showing how the combinations of Vossen and Denning and Nagar and Denning teach the subject matter recited in claims 2–4 and 18 and showing that a person of ordinary skill in the art would have been motivated to combine the teachings of these references in the manner asserted. *See* Pet. 27–36, 68–70.

Petitioner argues that a person of ordinary skill in the art would have been motivated to combine Denning’s access control teachings with the teachings of Vossen and with the teachings of Nagar “to provide a more finely-grained system for controlling access to files.” Pet. 27 (citing Ex. 1002 ¶ 106), 68 (citing Ex. 1002 ¶ 217); *see* Pet. 27–28 (citing advantages of Denning’s access control teachings and providing additional rationales for the combination of Vossen and Denning), 68–70 (citing

advantages of Denning’s access control teachings and providing additional rationales for the combination of Nagar and Denning).

Claim 2 recites, “The method according to claim 1, further comprising enforcing at least one policy.” Petitioner argues that Denning’s disclosure of enforcing an access control policy teaches this subject matter. Pet. 29 (citing Ex. 1006, 191; Ex. 1002 ¶¶ 110–116). As noted above, Denning discloses that “[a]n access control policy specifies the authorized accesses of a system” and that “an access control mechanism implements or enforces the policy.” Ex. 1006, 191.

Claim 3 recites, “The method according to claim 2, further comprising managing an operation in regards to said at least one policy.” Claim 4 depends from claim 3 and recites that “said operation comprises at least one of” multiple listed operations, including “reading a file” and “writing a file.” Petitioner argues that Denning’s disclosure of authorization lists that indicate the type of access that is permitted, such as read or write, teaches the subject matter of claims 3 and 4. Pet. 31–34 (citing Ex. 1006, 191–194, 196–200, 209–216, Fig. 4.12; Ex. 1002 ¶¶ 117–124). Denning discloses that authorization lists (or access-control lists) are “used to protect owned objects such as files” and that entries in these lists “indicate[] the type of access (read, write, or execute) permitted.” Ex. 1006, 209–211.

Claim 18 recites, “The method according to claim 1, wherein the allowing or denying said attempted operation further comprises identifying an attribute of data associated with said attempted operation.” Petitioner argues that “*Denning* associates subjects *s* (e.g., users) with access rights *r* (e.g., reading privileges) to objects *o* (e.g., files)” and denies the user access if the user lacks the requisite access rights. Pet. 35–36 (citing Ex. 1006,

192–193, 196–199, 207, 209–211, Fig. 4.1; Ex. 1002 ¶¶ 128–129). Denning discloses that an access matrix “lists the access **rights** (or privileges) of subject *s* for object *o*.” Ex. 1006, 192. Denning further discloses that a monitor “controls access to the object” and that “[t]he monitor for an object *o* prevents a subject *s* from accessing *o* when $A[s, o]$ does not contain the requisite right.” Ex. 1006, 193. Petitioner argues that Denning’s disclosure of using the access data to allow or deny an operation teaches that “the allowing or denying said attempted operation further comprises identifying an attribute of data associated with said attempted operation.” Pet. 35–36.

Patent Owner does not separately address Petitioner’s contentions as to claims 2–4 and 18 based on the combinations of Vossen and Denning and Nagar and Denning. *See generally* PO Resp.

We are persuaded by Petitioner’s contentions and evidence, discussed above, showing how the combinations of Vossen and Denning and Nagar and Denning teach the subject matter recited in claims 2–4 and 18 and showing why a person of ordinary skill in the art would have combined the teachings of Denning with the teachings of each of Vossen and Nagar. Having considered the full record developed during trial, we are persuaded by Petitioner’s contentions and evidence, and we determine that Petitioner has proven by a preponderance of the evidence that claims 2–4 and 18 of the ’524 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen and Denning and over the combined teachings of Nagar and Denning.

3. Claim 19 – Vossen and Denning

Claim 19 recites, “The method according to claim 1, further comprising creating at least one hash key to validate authenticity of said

portion of the storage medium.” Petitioner argues that Denning’s disclosure of using a hashing function to validate authenticity teaches this subject matter. Pet. 36–37 (citing Ex. 1006, 170–171, 224–225; Ex. 1002 ¶ 132). Denning discloses a “tree authentication scheme” in which “[a]ll entries in the public file are signed as a unit using a one-way hashing function.” Ex. 1006, 170. Denning explains that “[u]sers can authenticate their own keys” using “intermediate values of the hashing function,” which “form an **authentication path** of a tree, and serve as a form of certificate.” Ex. 1006, 170.

Petitioner contends that a person of ordinary skill in the art would have been motivated “to incorporate *Denning*’s hashing techniques into the control scheme of *Vossen*” to improve security in Vossen. Pet. 37 (citing Ex. 1002 ¶¶ 133–134). Petitioner also contends that Denning’s hashing functions would “enhance *Vossen*’s ability to detect malicious security breaches, a concern *Denning* already raises.” Pet. 38 (citing Ex. 1006, 191, 193, 206; Ex. 1002 ¶¶ 133–134).

Patent Owner does not separately address Petitioner’s contentions as to claim 19 based on the combination of Vossen and Denning. *See generally* PO Resp.

We are persuaded by Petitioner’s contentions and evidence, discussed above, showing how the combination of Vossen and Denning teaches the subject matter recited in claim 19 and showing why a person of ordinary skill in the art would have combined the teachings of Vossen and Denning. Having considered the full record developed during trial, we are persuaded by Petitioner’s contentions and evidence, and we determine that Petitioner has proven by a preponderance of the evidence that claim 19 of the ’524

patent is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen and Denning.

4. *Claim 19 – Nagar and Denning*

Petitioner’s reasons to combine Nagar and Denning focus on Denning’s teachings of access control. Pet. 68–70. Petitioner, however, does not explain how this reasoning applies to the subject matter of claim 19, which recites “creating at least one hash key to validate authenticity of said portion of the storage medium.” In arguing that claim 19 would have been obvious over Vossen and Denning, Petitioner explains that “[i]t would have been obvious to incorporate *Denning*’s hashing techniques into the control scheme of *Vossen*.” Pet. 37. But Petitioner does not explain why it would have been obvious to incorporate Denning’s hashing techniques with the teachings of Nagar. *See* Pet. 68–70.

Patent Owner does not separately address Petitioner’s contentions as to claim 19 based on the combination of Nagar and Denning. *See generally* PO Resp. Nevertheless, the burden remains on Petitioner to demonstrate unpatentability. 35 U.S.C. § 316(e); *see also Dynamic Drinkware LLC, v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). Because Petitioner relies on Denning to teach the subject matter recited in claim 19 but has not set forth articulated reasoning to combine the teachings of Nagar and Denning to arrive at this claimed subject matter, Petitioner has not proven, by a preponderance of the evidence, that claim 19 is unpatentable as obvious over the combination of Nagar and Denning.

*I. Obviousness over the Combinations of Vossen, Denning, and McGovern
and Nagar, Denning, and McGovern
(Claims 9, 11, 29–31)*

Petitioner asserts that claims 9, 11, and 29–31 of the '524 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen, Denning, and McGovern and the combined teachings of Nagar, Denning, and McGovern. Pet. 5–9, 38–53 (discussion of Vossen, Denning, and McGovern), 70–74 (discussion of Nagar, Denning, and McGovern).

1. McGovern

McGovern is a US patent publication titled “System and Method for Record Retention Date in a Write Once Read Many Storage System” and was published on May 5, 2005. Ex. 1007, codes (43), (54). Petitioner argues that the earliest possible priority date for claims 9, 11, and 29–31 is July 7, 2006, the filing date of the application for the '524 patent, because, according to Petitioner, none of the parent applications supports the “retention policy” subject matter recited in claims 9, 11 (through dependency from claim 9), and 29–31. Pet. 5–7. Therefore, Petitioner argues that McGovern is prior art under 35 U.S.C. § 102(b).

McGovern's May 5, 2005, publication date is more than one year before the July 7, 2006, filing date of the application for the '524 patent. Ex. 1001, code (22); Ex. 1007, code (43). Therefore, the burden of production was on Patent Owner to show support for the subject matter recited in claims 9, 11, and 29–31 in an earlier application to which the '524 patent claims priority. *See Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–28 (Fed. Cir. 2008) (discussing parties' respective burdens of production in the context of prior art and priority); *see also Dynamic*

Drinkware, 800 F.3d at 1378–1380 (discussing burdens of production in *inter partes* review). Patent Owner does not argue that any of claims 9, 11, and 29–31 are entitled to a priority date earlier than the filing date of the application for the '524 patent. *See generally* PO Resp. Therefore, we are persuaded by Petitioner's contention that McGovern qualifies as prior art under 35 U.S.C. § 102(b) to claims 9, 11, and 29–31.

McGovern discloses “providing a specified retention date within a data set that is locked against deletion or modification within a WORM [(write-once-read-many)] storage implementation.” Ex. 1007 ¶ 20.

2. Claims 9, 11, 29–31

Petitioner presents persuasive arguments and evidence showing how the combinations of Vossen, Denning, and McGovern and Nagar, Denning, and McGovern teach the subject matter recited in claims 9, 11, and 29–31 and showing that a person of ordinary skill in the art would have been motivated to combine the teachings of these references in the manner asserted. *See* Pet. 40–53, 70–74.

Claim 9 recites the following:

The method according to claim 2, wherein the policy comprises a retention policy comprising:

applying a restricted state to the portion of the storage medium;

preventing modification of the restricted state portion of the storage medium; and

associating a time of expiration with the restricted state portion of the storage medium.

Claim 11 recites, “The method according to claim 9, wherein preventing modification of the restricted state portion of the storage medium

comprises at least one of: . . .preventing deleting, preventing at least one form of modification.”

Petitioner argues that McGovern’s disclosure of committing data to a WORM status that prevents deletion or modification of the data until a retention date passes teaches this subject matter. Pet. 42–46 (citing, *inter alia*, Ex. 1007 ¶ 20). McGovern discloses “providing a specified retention date within a data set that is locked against deletion or modification within a WORM storage implementation. . . . Upon expiry of the retention date, the system allows deletion of the expired WORM file/data set.” Ex. 1007 ¶ 20.

Independent claim 29 is directed to “[a] computer program product for applying an operation access privilege to a storage medium, the computer program product including program logic, which when executed on a computer performs a method, the method comprising” steps similar to the limitations recited in claims 1, 2, and 9. Petitioner argues that it would have been obvious to implement the combinations of Vossen, Denning, and McGovern and Nagar, Denning, and McGovern as computer program products including program logic, which when executed on a computer performs a method, because “the entire purpose of each reference is to operate as instructions in a computer environment.” Pet. 48, 73. Petitioner argues that the remaining subject matter recited in claim 29 would have been obvious for the reasons set forth for claims 1, 2, and 9. Pet. 48–49, 73–74.

Claim 30 recites,

The computer program product of claim 29, wherein the retention policy comprises: determining the restricted state portion of the storage medium is in an unexpired restricted state when the associated time of expiration is associated with at least one of: a fixed point in time in the future, an indefinite time of expiration, or an infinite time of expiration; and preventing

modification of the unexpired restricted state portion of the storage medium.

Petitioner contends McGovern's disclosure of locking data in a restricted WORM state such that "[n]o modification or deletion of files is permitted until an applicable retention date expires" (Ex. 1007 ¶ 21) teaches this subject matter. Pet. 50, 74.

Claim 31 recites,

The computer program product of claim 29, wherein the retention policy comprises: determining the restricted state portion of the storage medium is in an expired restricted state when the associated time of expiration is associated with a fixed time of expiration in the past; preventing modification of the expired restricted state portion of the storage medium; and allowing deletion of the expired restricted state portion of the storage medium.

Petitioner contends McGovern's disclosure of allowing limited action on data, such as only deleting a file, after the retention date passes teaches this subject matter. Pet. 52 (citing Ex. 1007 ¶ 140, Fig. 15; Ex. 1002 ¶ 172), 74. For example, McGovern discloses that when the retention date has passed, "the user or administrator is permitted to take limited action on the file, or action is automatically taken. In an illustrative embodiment, that action is typically limited only to deletion of the file from the volume" Ex. 1007 ¶ 140.

Petitioner provides various articulated reasons for why a person of ordinary skill in the art would have been motivated to combine McGovern's WORM retention teachings with the combination of Vossen and Denning and the combination of Nagar and Denning, including "to provide additional functionality for controlling access to files," and Petitioner argues that McGovern's disclosure that governmental regulations sometimes compel

retention procedures supports Petitioner's assertion that it would have been obvious to implement McGovern's retention procedures. Pet. 40–42 (citing, *inter alia*, Ex. 1002 ¶¶ 136–141; Ex. 1007 ¶¶ 10, 15, 20–21, 79, 120–121), 70–72; *see* Ex. 1007 ¶ 10 (describing Security and Exchange Commission rule requiring brokers and investment institutions to store certain records unchanged for a number of years).

Apart from its arguments for limitations of independent claim 29 that are also in claim 1, which we address above, Patent Owner does not separately address Petitioner's contentions as to claims 9, 11, and 29–31 based on the combinations of Vossen, Denning, and McGovern and Nagar, Denning, and McGovern. *See generally* PO Resp.

We are persuaded by Petitioner's contentions and evidence, discussed above, showing how the combinations of Vossen, Denning, and McGovern and Nagar, Denning, and McGovern teach the subject matter recited in claims 9 and 11 and showing why a person of ordinary skill in the art would have combined the teachings of the references in the manner asserted. Having considered the full record developed during trial, we are persuaded by Petitioner's contentions and evidence, and we determine that Petitioner has proven by a preponderance of the evidence that claims 9 and 11 of the '524 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen, Denning, and McGovern and over the combined teachings of Nagar, Denning, and McGovern.

*J. Obviousness over the Combinations of Vossen and Kung and
Nagar and Kung
(Claim 24)*

Petitioner asserts that claim 24 of the '524 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen

and Kung and the combined teachings of Nagar and Kung. Pet. 5–9, 53–56 (discussion of Vossen and Kung), 74–76 (discussion of Nagar and Kung).

Claim 24 recites, “The method according to claim 1, further comprising forcing a secure erasure for a delete operation on said at least a portion of the storage medium, wherein secure erasure comprises overwriting the contents of said at least a portion of the storage medium.”

Petitioner argues that Kung discloses secure erasure by overwriting data with 0s and 1s and by using encryption. Pet. 53–54 (citing Ex. 1008, 1:5–10, 1:12–16, 1:24–27, 3:18–62; Ex. 1002 ¶¶ 68–70). Kung discloses that a

conventional method of file deletion requires a user to overwrite 0’s and 1’s over the entire data file as to remove any magnetic remnants of the removed information. This method is slow because the system must write 0’s and 1’s many times to ensure that the stored information cannot be recovered.

Ex. 1008, 1:24–29. Kung further discloses the following:

In the one way deletion mode 17, wherein the user does not expect to “undelete” the data, a one-way encryption algorithm is used to increase the speed of secure deletion of the file 20. In the one way mode 17, the data in the file 20 is encrypted using a random external key 21, and then the key 21 is automatically destroyed 19 and cannot be used to recover the data.

Ex. 1008, 3:36–45.

Petitioner argues that a person of ordinary skill in the art “would have been motivated to implement the deletion methods discussed in *Kung* within *Vossen*’s system to provide additional security for erased files.” Pet. 54 (citing Ex. 1002 ¶¶ 175–178). Similarly, Petitioner argues that a person of ordinary skill in the art “would have been motivated to combine *Kung*’s secure file-erasure method with *Nagar*’s filter drivers, as this combination

would improve the system’s ability to restrict unauthorized access to a deleted file,” and also would have been motivated “to provide heightened security to its file system, such as preventing a hacker from accessing the content of a deleted file.” Pet. 74–75 (citing Ex. 1002 ¶¶ 248–249).

Petitioner contends that combining Kung’s teachings with Vossen and with Nagar would have been within the skill of a person of ordinary skill in the art. Pet. 54 (citing Ex. 1002 ¶ 175), 75 (citing Ex. 1002 ¶¶ 250, 252).

Patent Owner argues that Petitioner’s argument based on Kung’s disclosure of the “conventional method” of overwriting data with 0s and 1s fails “because Kung teaches away from using this approach.” PO Resp. 38. Although Kung describes this technique as “slow” and proposes other techniques for secure erasure as improvements, we do not view this as teaching away from this method of secure erasure. As the Federal Circuit has stated, “a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.” *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006). “Instead, the benefits, both lost and gained, should be weighed against one another.” *Id.* (quoting *Winner Int’l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 n.8 (Fed. Cir. 2000)). Kung itself discloses that a benefit to this technique is that it “ensure[s] that the stored information cannot be recovered.” Ex. 1008, 1:27–29. Thus, Kung’s express disclosure supports Petitioner’s proposed motivation to combine—to enhance security. *See* Pet. 54 (citing Ex. 1002 ¶¶ 175–178). We do not find Kung’s disclosure of a drawback to this approach—slower speed—as outweighing the benefits it teaches of secure erasure. Furthermore, for the reasons explained below, we

find Kung's technique for secure erasure via encryption teaches the claimed subject matter.

Furthermore, we do not agree that Petitioner's contention based on Kung's disclosure of overwriting data with 0s and 1s "is based on an identity of a user," as asserted by Patent Owner. *See* PO Resp. 38. Patent Owner's argument appears to be based on Kung's disclosure that this method "requires a user to overwrite 0's and 1's over the entire data file as to remove any magnetic remnants of the removed information." Ex. 1008, 1:24–27, *quoted in* PO Resp. 38. In the next sentence, however, Kung states that "the system must write 0's and 1's many times to ensure that the stored information cannot be recovered." Ex. 1008, 1:27–29. Thus, this is a process performed by the system.

As to Petitioner's arguments based on Kung's secure erasure using encryption, Patent Owner argues that, for the one-way deletion approach in which an encryption key is provided externally, the encryption key continues to exist externally even after it is destroyed internally, thus making recovery of the data still possible. PO Resp. 36–37 (citing Ex. 1008, 3:33–62, Figure; Ex. 2001 ¶ 78). Patent Owner argues, therefore, that "regardless of whether a key may be retrieved to read the file, the content remains on the storage medium and is not overwritten." PO Resp. 37 (citing Ex. 2001 ¶ 78). Kung, however, discloses that, in the one way deletion mode, "the key 21 is automatically destroyed 19 and cannot be used to recover the data. Consequently without the key 21, the data cannot be decrypted and is thus unreadable by anyone." Ex. 1008, 3:40–45. Kung's express disclosure, therefore, states that the key is destroyed and that the data cannot be recovered by anyone, contradicting Patent Owner's argument and Dr.

Melendez’s testimony on this point. Based on Kung’s disclosure that the key is destroyed, we also disagree with Patent Owner’s argument that Kung’s one way encryption approach does not overwrite data, which is also based on the premise that an encryption key still exists that can be used to recover the data. *See* PO Resp. 38–39 (citing Ex. 2001 ¶ 79; Ex. 1008, code (57), 1:64–66, 2:3–8, 2:36–40, 3:43–45, 3:50–58, 4:3–7, Figure).

We are persuaded, and we find, that Kung’s disclosures of secure erasure by overwriting data with 0s and 1s and by one way deletion using encryption teach the subject matter recited in claim 24 because both perform secure erasure by overwriting contents of the storage medium—the first by overwriting with 0s and 1s and the second by overwriting with an encrypted form of the data. Ex. 1008, 1:24–27, 3:36–45, Figure. We also are persuaded, and we find, that a person of ordinary skill in the art would have been motivated to combine Kung’s secure erasure teachings with the teachings of each of Vossen and Nagar to improve security. Ex. 1002 ¶¶ 175–178, 248–252.

Furthermore, the ’524 patent states that “[s]ecure erasure is a required by such compliance requirements such as DOD [(Department of Defense)] 5015.2 which require that file contents that are being deleted to be overwritten with random patterns that would ensure that they could never be restored.” Ex. 1001, 16:44–48, *quoted in* PO Resp. 35. We find that government regulations expressly requiring secure erasure provide further motivation (out of necessity in some circumstances) for a person of ordinary skill in the art to combine secure erasure teachings with the teachings of Vossen and Nagar. *See Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1339 (Fed. Cir. 2020) (“[I]t is appropriate to rely on admissions in a

patent's specification when assessing whether that patent's claims would have been obvious."'). Here, the additional subject matter recited in claim 24 simply covers what the '524 patent acknowledges was already required by a government regulation before the filing of the application for the '524 patent.

Having considered the full record developed during trial, we are persuaded by Petitioner's contentions and evidence, and we determine that Petitioner has proven by a preponderance of the evidence that claim 24 of the '524 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over the combined teachings of Vossen and Kung and over the combined teachings of Nagar and Kung.

K. Constitutionality

Patent Owner asserts that *inter partes* review proceedings are "unconstitutional under the Takings Clause . . . and Due Process Clause . . . of the United States Constitution, as applied retroactively to this patent which issued before" *inter partes* review proceedings became law. PO Resp. 39.

Petitioner correctly notes the following:

Recent Federal Circuit cases foreclose these arguments. Applying *inter partes* review to pre-AIA patents is not an unconstitutional taking. *See Celgene Corp. v. Peter*, 931 F.3d 1342, 1358-63 (Fed. Cir. 2019). Nor does it upset due process. *See OSI Pharm., LLC v. Apotex, Inc.*, 939 F.3d 1375, 1385-86 (Fed. Cir. 2019). Petitions to upend these rulings have uniformly failed. *See, e.g., Enzo Life Scis., Inc. v. Becton, Dickinson & Co.*, 780 Fed. Appx. 903, 911 (Fed. Cir. 2019). Unless the Supreme Court reverses these cases, they remain controlling law.

Pet. Reply 26.

We decline to consider Patent Owner's arguments because the Federal Circuit has determined that *inter partes* review proceedings are not unconstitutional under the Takings Clause or Due Process Clause. *Celgene*, 931 F.3d at 1362; *Arthrex, Inc. v. Smith & Nephew, Inc.*, 935 F.3d 1319, 1331–32 (Fed. Cir. 2019).

III. CONCLUSION¹²

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, that the challenged claims are unpatentable, as summarized in the following table:

Claims	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1	102(e)	Vossen	1	
1	103(a)	Vossen	1	
2–4, 18, 19	103(a)	Vossen, Denning	2–4, 18, 19	
9, 11, 29–31	103(a)	Vossen, Denning, McGovern	9, 11, 29–31	
24	103(a)	Vossen, Kung	24	
1	102(b)	Nagar	1	
1	103(a)	Nagar	1	
2–4, 18, 19	103(a)	Nagar, Denning	2–4, 18	19
9, 11, 29–31	103(a)	Nagar, Denning, McGovern	9, 11, 29–31	
24	103(a)	Nagar, Kung	24	
Overall Outcome			1–4, 9, 11, 18, 19, 24, 29–31	

¹² Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IV. ORDER

Accordingly, it is:

ORDERED that claims 1–4, 9, 11, 18, 19, 24, and 29–31 of the '524 patent have been shown to be unpatentable; and

FURTHERED ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2019-00604
Patent 7,536,524 B2

PETITIONER:

Erika Arner
Joshua Goldberg
Jason Stach
Cory Bell
Benjamin Saidman
Andrew Devkar
Diek Van Nort
erika.arner@finnegan.com
joshua.goldberg@finnegan.com
jason.stach@finnegan.com
cory.bell@finnegan.com
benjamin.saidman@finnegan.com
andrew.devkar@morganlewis.com
dvannort@mofo.com

PATENT OWNER:

Gregory S. Donahue
Andrew DiNovo
gdonahue@dpelaw.com
adinovo@dpelaw.com