UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NetApp, Inc.,
Petitioner,

v.

KOM Software, Inc.,
Patent Owner.

Case IPR2019-00608
Patent 9,361,243

PATENT OWNER'S NOTICE OF APPEAL

Mail Stop
Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to 35 U.S.C. §§ 141 and 142 and 37 C.F.R. § 90.2(a), Patent Owner KOM Software, Inc. ("Patent Owner") hereby provides notice that it appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision of the Patent Trial and Appeal Board ("Board") entered September 22, 2020 (Paper 32), and from all underlying findings, orders, decisions, rulings, and opinions regarding U.S. Patent No. 9,361,243 ("the '243 patent") in *Inter Partes* Review IPR2019-00608.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Patent Owner states that the issues for appeal include, but are not limited to: the Board's determination that claims 1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, and 96 of the '243 patent have been shown by a preponderance of the evidence to be unpatentable and any other finding, evidence, or determination supporting or related to that determination, as well as all other issues decided adversely to Petitioner in any orders, decisions, rulings, or opinions.

A copy of the decision being appealed is attached to this Notice.

Pursuant to 35 U.S.C. § 142 and 37 C.F.R. § 90.2(a), this Notice is being filed with the Director of the United States Patent and Trademark Office. Simultaneous with this submission, a copy of this Notice is being filed with the Patent Trial and Appeal Board. In addition, a copy of this Notice, along with the required docketing

fee, is being filed with the Clerk's office of the United States Court of Appeals for the Federal Circuit via CM/ECF.

Date: November 23, 2020

Respectfully Submitted,

/s/ *Wenye Tan*

Wenye Tan
Reg. No. 55,662
Xiaoqun Wu
Reg. No. 54,553
Anova Law Group PLLC
21495 Ridgetop Circle, Suite 300
Sterling, VA 20166
Telephone: 571.379.9468
Facsimile: 703.935.1394

Counsel for Patent Owner
KOM Software, Inc.

CERTIFICATE OF FILING AND SERVICE

The undersigned certifies that, in addition to being filed electronically through the Patent Trial and Appeal Board's E2E, the foregoing Notice of Appeal was filed and served by Express Mail on November 23, 2020, with the Director of the United States Patent and Trademark Office, at the following address:

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
P.O. Box 1450
Alexandria, VA 22313-1450

The undersigned certifies that a copy of the foregoing Notice of Appeal, along with the required docket fee, was filed on November 23, 2020, with the Clerk's Office for the United States Court of Appeals for the Federal Circuit through the Court's CM/ECF filing system.

The undersigned certifies service pursuant to 37 C.F.R. § 42.6(e) of a copy of this Notice of Appeal by electronic mail on November 23, 2020, on the counsel of record for Petitioners at the following addresses:

Erika H Arner, erika.arner@finnegan.com
Jason E. Stach, jason.stach@finnegan.com
Joshua Goldberg, joshua.goldberg@finnegan.com
Guang-Yu Zhu, guang-yu.zhu@finnegan.com
Cory Bell, cory.bell@finnegan.com
Diek Van Nort, dvannort@mofo.com

Dated: November 23, 2020

By: /s/ *Wenye Tan*

Wenye Tan
Reg. No. 55,662
Xiaoqun Wu
Reg. No. 54,553
Anova Law Group PLLC
21495 Ridgetop Circle, Suite 300
Sterling, VA 20166
Telephone: 571.379.9468
Facsimile: 703.935.1394

Counsel for Patent Owner
KOM Software, Inc.

Trials@uspto.gov
571-272-7822

Paper 32
September 22, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETAPP, INC.,
Petitioner,

v.

KOM SOFTWARE, INC.,
Patent Owner.

IPR2019-00607
IPR2019-00608
Patent 9,361,243 B2

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

McGRAW, *Administrative Patent Judge*.

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

I. INTRODUCTION

In *inter partes* review IPR2019-00607, NetApp, Inc. ("Petitioner")[1] challenges the patentability of claims 1–4, 16, 24–26, 32–37, 39, 54–57, 61–63, 66–69, 81, 87–89, 93–95, and 101–103 of U.S. Patent No. 9,361,243 B2 ("the '243 patent," Ex. 1001[2]), which is assigned to KOM Software, Inc. ("Patent Owner"). Paper 3 ("Pet."). In *inter partes* review IPR2019-00608, Petitioner challenges the patentability of claims 1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, and 96 of the '243 patent. IPR2019-00608, Paper 3 ("IPR608-Pet.").

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 trials in these *inter partes* review proceedings. For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that claims 1–3, 6–8, 10–12, 14, 17, 21, 24, 25, 27, 32, 33, 35–37, 39, 54–57, 61–63, 65–68, 71–73, 75–77, 79, 82, 86–89, 93, 94, 96, 101, and 102 of the '243 patent are unpatentable, but has not shown by a preponderance of the evidence that claims 4, 34, 69, 103 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.").

[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 25.

[2] Unless otherwise indicated, citations are to papers filed in IPR2019-00607. Similar papers are filed in IPR2019-00608.

A. Procedural History

On January 28, 2019, Petitioner filed a Petition for *inter partes* review of claims 1–4, 16, 24–26, 32–37, 39, 54–57, 61–63, 66–69, 81, 87–89, 93–95, and 101–103 of the '243 patent in IPR2019-00607. Pet. 14, 53, 66. On the same day, Petitioner filed a Petition for *inter partes* review of 1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, and 96 of the '243 patent. IPR608-Pet. Patent Owner filed a Preliminary Response in each proceeding. Paper 9 ("Prelim. Resp."); IPR2019-00608, Paper 9 ("IPR608-Prelim. Resp."). Trial was instituted on all grounds of unpatentability. Paper 10 ("Inst. Dec."), 27; IPR2019-00608, Paper 10 (IPR608-Inst. Dec."), 30.

Following institution, in each proceeding, Patent Owner filed a Response (Paper 14, "PO Resp."; IPR2019-00608, Paper 14 ("IPR608-PO Resp.")), Petitioner filed a Reply (Paper 23, ("Reply"); IPR2019-00608, Paper 23 ("IPR608-PO Resp.")), and Patent Owner filed a Sur-reply (Paper 28, "PO Sur-reply"; IPR2019-00608, Paper 28 ("IPR608-PO Sur-resp.")). A consolidated oral hearing was held on June 18, 2020 for both proceedings, a transcript of which appears in the record. Paper 31 ("Tr.").

B. Related Matters

Petitioner identifies the following pending litigations involving the '243 patent: (1) *KOM Software Inc. v. Hitachi Vantara Corp.*, Case No. 1-18-cv-00158 (D. Del.); (2) *KOM Software Inc. v. Hewlett Packard Enterprise Co.*, Case No. 1-18-cv-00159 (D. Del.); and (3) *KOM Software Inc. v. NetApp, Inc.*, Case No. 1-18-cv-00160 (D. Del.). Pet. 73; Paper 4, 3. Additionally, the parties identify numerous other *inter partes* review

proceedings relating to other patents owned by the Patent Owner. *See, e.g.,* Pet. 73; Paper 4, 2–3; Paper 8, 2–3.

C. Real Parties-in-Interest

Petitioner identifies NetApp, Inc. and Hewlett Packard Enterprise Company and Patent Owner identifies KOM Software, Inc. as the real parties-in-interest. Pet. 73; Paper 4, 2; Paper 8, 2.

D. The '243 Patent

The '243 patent, titled "Method and System for Providing Restricted Access to a Storage Medium," relates generally to a method of providing restricted write access on a data storage medium. Ex. 1001, code (54), 1:33–35; *id.* at 1:45–48 (describing "access privileges including read and write privileges"). The '243 patent states that access privileges provided by previous operating systems "fail to adequately provide protection for archival storage devices such as magnetic tape or removable optical media." *Id*. at 1:49–51. For example, "[w]hen an archive data store is used with a data store device, it is often desirable that it not be written to." *Id*. at 2:33–34. However, when a data store device is accessed, file systems of previous operating systems may perform updating of file access information even when it is not desired. *Id*. at 2:34–39. To solve this problem, the '243 patent discloses, *inter alia*, an operating system that includes a "trap layer" or "filter layer" disposed between the application layer and the file system layer. *Id*. at 13:20–22. Figure 3, reproduced below, illustrates a block diagram of an operating system that includes a trap layer.

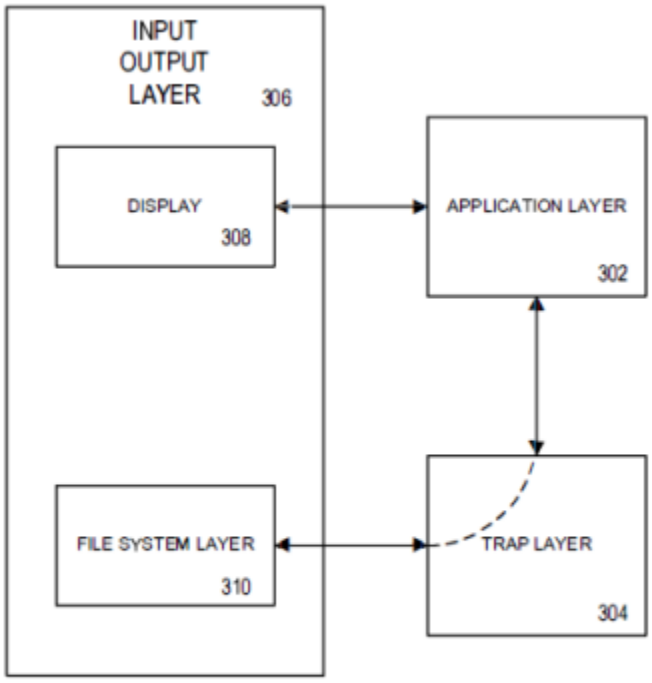

FIG. 3

Figure 3 above illustrates an operating system that includes application layer 302 that communicates with input output layer 306. Ex. 1001, 13:11–15. Input output layer 306 may include display 308 and file system layer 310. *Id.* at 13:15–17. Application layer 302 communicates with file system layer 310 to perform read and write operations with storage media. *Id.* at 13:18–20. Trap layer 304 (also referred to as a filter layer) is disposed between application layer 302 and file system layer 310. *Id.* at 13:20–22. Each file system access request that is transmitted from the application layer to the file system layer is intercepted by the trap layer, where restrictions relating to access privileges are implemented. *Id.* at 13:23–27. Some access requests are blocked and error messages are returned to the application layer, and some access requests may be modified and passed on to the file system in modified form. *Id.* at 13:28–35.

Figure 5, reproduced below, illustrates a flow diagram of a method of storing data in a storage medium applying a trap layer as in Figure 3.

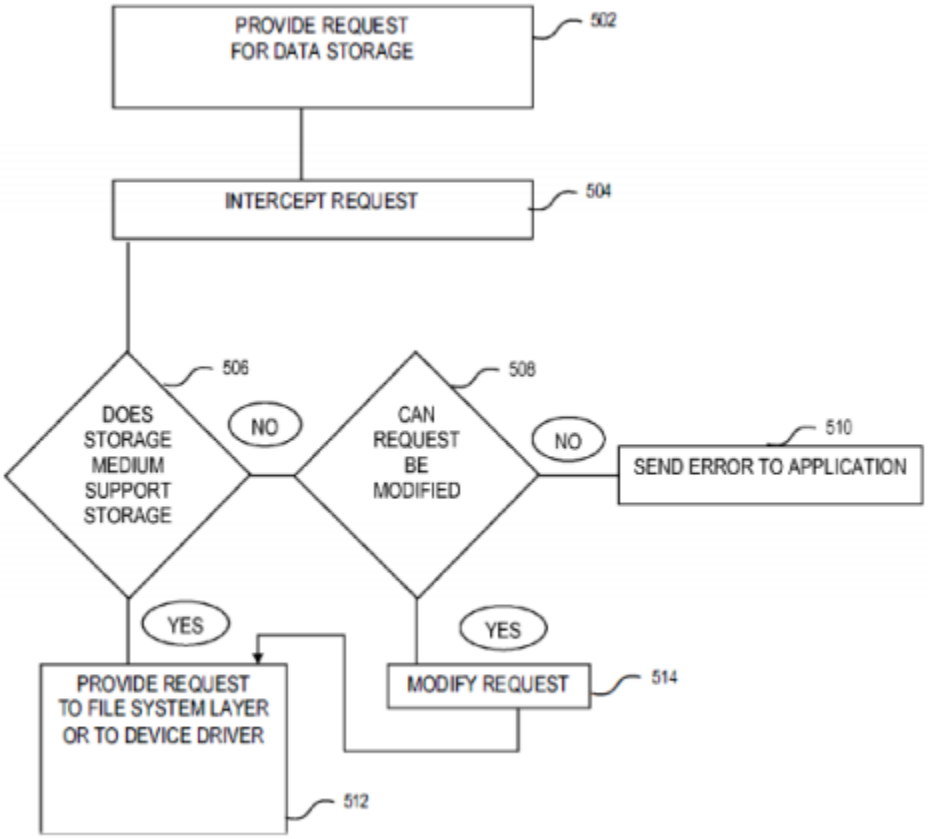

FIG. 5

Figure 5 above is a flow diagram including step 502, in which an application layer (e.g., 302 discussed *supra*) may seek to store data on a storage medium by communicating with a file system layer (e.g., 310 discussed *supra*). Ex. 1001, 15:27–37. A trap layer (e.g., 304 discussed *supra*) intercepts the request at step 504 and, at step 506, determines whether the storage medium supports the request to store data. *Id*. at 15:37–39. If step 506 determines the storage medium supports the request to store data, step 512 passes the request on to the file system layer for normal processing. *Id*. at 15:40–42. If step 506 determines the storage medium does not support the request to store data, step 508 determines whether the request can be

modified to allow the requested access, and if so, step 514 modifies the request and forwards the modified request to step 512 for further processing. *Id*. at 15:42–47. If step 508 determines the unsupported request cannot be appropriately modified, step 510 returns a corresponding error indication to the application layer. *Id*. at 15:47–53.

E. Illustrative Claim

Of the challenged claims, claims 1, 62, 66 are independent. Claim 1 is illustrative and is reproduced below, with bracketed material and formatting added for clarity.

> 1. [a] A computer implemented method for applying, by at least one computer processor, a computer file system operation access privilege to a computer storage medium, comprises:
>
> [b] associating, by the at least one computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium;
>
> [c] intercepting, by the at least one computer processor, by at least one computer file system trap layer or at least one file system filter layer, an attempted operation on said at least a portion of the computer storage medium,
>
> [d] wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation;
>
> [e] comparing, by the at least one computer processor, the attempted operation to the computer file system operation access privilege; and
>
> [f] allowing, or denying, by the at least one computer processor, the attempted operation based on the comparing

> the attempted operation to the computer file system operation access privilege.

Ex. 3002 (Certificate of Correction), 1.[3]

F. Asserted Challenges to Patentability

In IPR2019-00607, Petitioner asserts that claims 1–4, 16, 24–26, 32–37, 39, 54–57, 61–63, 66–69, 81, 87–89, 93–95, and 101–103 are unpatentable based on the following challenges:

Claims Challenged	35 U.S.C. §[4]	Reference(s)/Basis
1–4, 24, 25, 32–37, 39, 54–57, 61–63, 66–69, 87–89, 93, 94, 101–103	102(a)	Nagar[5]
1–4, 24, 25, 32–37, 39, 54–57, 61–63, 66–69, 87–89, 93, 94, 101–103	103	Nagar
16, 26, 81, 95	103	Nagar, Kung[6]

In IPR2019-00608, Petitioner asserts that claims 1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, and 96 are unpatentable based on the following challenges:

[3] A Certificate of Correction (Ex. 3002) issued on April 23, 2019 to correct claims 1–5 to reflect claim amendments that were made during prosecution but that were not included in the originally issued patent. *See* Ex. 3001, 1.

[4] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) ("AIA"), amended 35 U.S.C. §§ 102 and 103. Because the challenged claims of the '243 patent have an effective filing date before the effective date of the applicable AIA amendments, we refer to the pre-AIA versions of §§ 102 and 103.

[5] RAJEEV NAGAR, WINDOWS NT FILE SYSTEM INTERNALS: A DEVELOPER'S GUIDE (1997) (Ex. 1005, "Nagar").

[6] US 5,265,159, issued Nov. 23, 1993 (Ex. 1008, "Kung").

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 62, 66[7]	102(a)	Nagar
6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 82, 86, 96	103	Nagar, McGovern[8]
18, 19, 83, 84	103	Nagar, Vossen[9]
5, 20, 64, 70, 85	103	Nagar, Denning[10]

G. Testimonial Evidence

In each proceeding, Petitioner relies on a declaration by Jon B. Weissman, Ph.D. (Ex. 1002; IPR2019-00608, Ex. 1002) and Patent Owner relies on a declaration by Jose Luis Melendez, Ph.D. (Ex. 2001; IPR2019-00608, Ex. 2001).

II. ANALYSIS

A. Principles of Law

To prevail on its challenge to Patent Owner's claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e) (2012); 37 C.F.R. § 42.1(d) (2018). The petitioner "has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring

[7] Petitioner presents the same Nagar based anticipation and obviousness arguments for independent claims 1, 62, and 66 in both IPR2019-00607 and IPR2019-00608. *See* IPR608-Pet.19 n.3.
[8] US Patent Publication No. 2005/0097260 A1 (Ex. 1006 "McGovern")..
[9] US 6,026,402 (Ex. 1007, "Vossen").
[10] Dorothy Elizabeth Robling Denning, CRYPTOGRAPHY AND DATA SECURITY, (1982) (Ex. 1013, "Denning").

inter partes review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

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, 1369 (Fed. Cir. 2008); *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001). Each element of the challenged claim must be found, either expressly or inherently, in the single prior art reference. *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987). While 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); *In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990). Thus, the dispositive question is whether one skilled in the art would reasonably understand or infer from a prior art reference that every claim element is disclosed in that reference. *Eli Lilly v. Los Angeles Biomedical Research Inst. at Harbor–UCLA Med. Ctr.*, 849 F.3d 1073, 1074–75 (Fed. Cir. 2017). Still further, "it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom." *In re Preda*, 401 F.2d 825, 826 (CCPA 1968).

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.[11] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner contends a person of ordinary skill at the time of the invention of the '243 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 ¶ 35).

In its Patent Owner Response, Patent Owner provides a slightly different definition from that proposed by Petitioner, 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. 11–12 (citing Ex. 2001 ¶ 35). Patent Owner' declarant, Dr. Melendez, also provides a slightly different definition, stating that a POSITA may also

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

have a degree in electronics engineering or applied mathematics. *See, e.g.,* Ex. 2001 ¶ 35.

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 (or a degree in electronics engineering or applied mathematics as asserted by Dr. Melendez) 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.

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.

Rather, both parties contend that the other party's declarant is not a person of ordinary skill in the art. Petitioner contends Patent Owner's expert, Dr. Melendez, does not have experience in the relevant field of data storage management and that Patent Owner has not demonstrated that Dr. Melendez is one of ordinary skill, let alone an expert in the field of data storage management. Reply 5–6, 23–25. Patent Owner contends Petitioner's expert, Dr. Weissman, is "a person with a high degree of expertise in the art rather than ordinary skill" and that "Dr. Weissman's opinions of what a person of ordinary skill would think should accordingly not be relied upon, because there is no way to ascertain if that opinion would remain his opinion if the skill was actually ordinary." PO Sur-reply 10.

Based on the record before us, including the types of problems and solutions described in the '243 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' or Dr. Melendez's definition.

Regarding the parties' arguments that the other party's expert is not a person of ordinary skill in the art, the law does not require that a declarant must actually be a person of ordinary skill in the art in order to present testimony as to what a person of ordinary skill in the art would have understood at the time of the invention. *See, e.g.*, *SEB S.A. v. Montgomery Ward & Co. Inc.*, 594 F.3d 1360, 1373 (Fed. Cir. 2010) (stating there is no requirement of a perfect match between an expert's experience and the field of the art in question, provided the expert has "sufficient relevant technical experience" to testify). The Federal Circuit has explained that a person of ordinary skill in the art is a "hypothetical person postulated by § 103" that is "presumed to have . . . knowledge of all material prior art." *Kimberly-Clark Corp. v. Johnson & Johnson*, 745 F.2d 1437, 1452–53 (Fed. Cir. 1984); *see also id.* at 1454 ("It should be clear that that hypothetical person [of ordinary skill in the art] is not the inventor, but an imaginary being possessing 'ordinary skill in the art' created by Congress to provide a *standard of patentability* . . . .").

Thus, the proper question to ask is not whether the testifying witness is in fact such a "hypothetical person," but rather whether the testifying witness possesses sufficient qualifications to be able to testify as to what the

hypothetical person of ordinary skill in the art postulated by § 103 would have known and understood at the time of the invention.

We determine both declarants have sufficient qualifications to be able to testify as to what the hypothetical person of ordinary skill in the art would have known and understood at the time of the invention.[12] We disagree with Patent Owner that we should accord little or no weight to Dr. Weissman's opinions because it cannot be determined which opinions are offered are a result of Dr. Weissman's allegedly unusually high level of expertise. *See, e.g.,* PO Sur-reply 10. Dr. Weissman testified that he considered the level of skill when rendering his opinion. *See, e.g.,* Ex. 1002 ¶¶ 29–31, 35–36.

We also disagree with Petitioner that Dr. Melendez lacks sufficient experience in data storage management such that his testimony should be accorded little to no weight. *See, e.g.,* Reply 5–6, 23–25. Dr. Melendez holds a Doctor of Philosophy in Electrical Engineering from Stanford University and a Master of Science in Electrical Engineering and Computer Science as well as a Bachelor of Science in Electrical Engineering from Massachusetts Institute of Technology. Ex. 2001 ¶ 19. Dr. Melendez is currently a Professor of Computer Science and Engineering at the University of Puerto Rico at Mayagüez, where he develops and teaches courses and defines and conducts research related to computer science. *Id.* ¶ 18. Additionally, Patent Owner explains that Dr. Melendez specifically worked on data storage systems including while working at Texas Instruments (1999-2001). *See* PO Sur-reply 22 (citing Ex. 2001 ¶ 22). As such, we find Dr. Melendez has sufficient qualifications to be able to testify as to what the

[12] As noted above, the obviousness analysis would be same under all proposed definitions of a POSITA.

hypothetical person of ordinary skill in the art would have known and understood at the time of the invention.

C. Claim Interpretation

In an *inter partes* review filed after November 13, 2018, such as here, we construe the claims 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, 51,340, 51,358 (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)). Under this standard, claim terms are given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Philips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc). If the specification "reveal[s] a special definition given to a claim term by the patentee that differs from the meaning it would otherwise possess[,] . . . the inventor's lexicography governs." *Id.* at 1316 (Fed. Cir. 2005). We construe the claims in accordance with these principles.

1. "associating, by the at least one computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium"

Although both parties assert that none of the claim terms needs to be expressly construed (*see* Pet. 9; PO Resp. 13), the parties dispute the meaning of the "associating" step recited in claim element 1[b] (i.e., "associating, by the at least one computer processor, the computer file

system operation access privilege with at least a portion of the computer storage medium") and similarly recited in independent claims 62 and 66.

Patent Owner argues that the associating step requires that "the storage medium itself maintains its associated operation access privileges—independent of the computer" such that "the associated privileges follow the medium when it is used on other computers." PO Resp. 17–19 (citing Ex. 1001, 15:64–16:7, Fig. 6; Ex. 2001 ¶¶ 41, 43). Patent Owner further contends that "[p]rivileges associated with the medium within the '243 patent are persistent, and would necessarily follow the medium from where they may be loaded when mounted." PO Sur-reply 4. Patent Owner also contends the '243 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. 4–5 (citing Ex. 1001, 15:64–16:7; Ex. 2001 ¶ 37). During oral argument, Patent Owner stated that the purpose of the invention is to have a "persistent association of" "operation access privileges" "with a particular storage medium" and that "the only embodiment of association" depicted in the '243 patent states the "storage medium may have stored thereon data relating to access privileges for the storage medium." Tr. 32:6–17.

Thus, Patent Owner contends the operation access privileges must be stored or maintained on the storage medium so that the privileges are "persistent" and therefore would follow the storage medium, such that they may be loaded from the storage medium when the storage medium is mounted.

Petitioner responds that Patent Owner is attempting improperly to read limitations from a preferred embodiment into the claims. *See* Reply 2–4.

We agree with Petitioner.

The plain and ordinary meaning of the phrase "associating, by [a] computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium" does not mean that the access privilege *must* be stored or maintained on the computer storage medium or that the access privileges associated with the storage medium are persistent and would *necessarily* follow the storage medium from where they may be loaded when the storage medium is mounted. The plain and ordinary meaning of "associating" does not require "storing" or "maintaining." The independent claims do not recite "store" or "maintain" or otherwise indicate that the access privilege must be stored on the computer storage medium or otherwise persistently maintained on the computer storage medium even if the medium is dismounted from a computer, as proposed by Patent Owner.

Moreover, Patent Owner's construction—requiring that the "storage medium itself maintains its associated operation access privileges—independent of the computer" (PO Resp. 18–19)—is inconsistent with the claim language itself, which requires the *computer processor* to associate the access privilege with the storage medium. *See* Ex. 3002, 1 (stating "associating, *by the at least one computer processor*, the computer file system operation access privilege with at least a portion of the computer storage medium"). Thus, the plain meaning of a claim term that requires the association of an operation access privilege with a storage medium by a

computer processor is not that the storage medium must maintain its associated operation access privileges independent of the computer processor.

Nor does the specification clearly set forth or otherwise support the definition of the "associating" term proposed by Patent Owner. Patent Owner cites to the disclosure of the '243 patent pertaining to Figure 6, which is reproduced below. *See, e.g.,* PO Resp. 4–5, 17–19; PO Sur-reply 4–5.

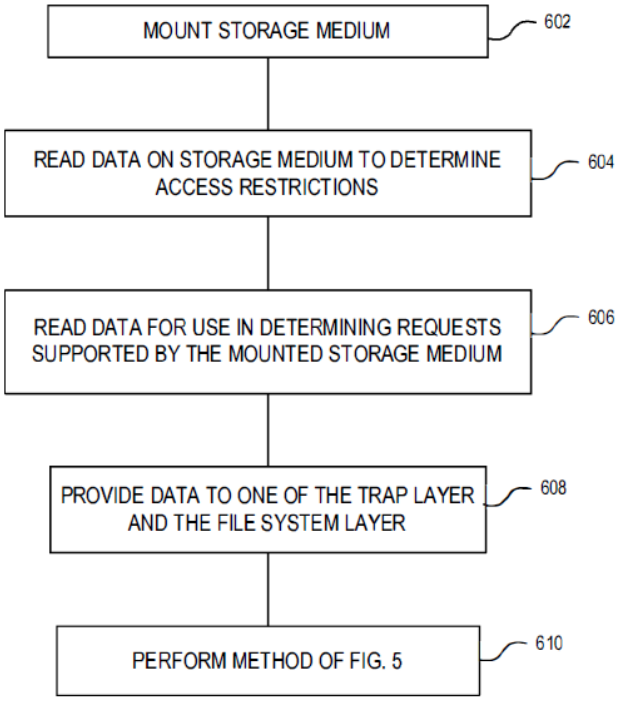

FIG. 6

Figure 6 of the '243 patent, reproduced above, is "a simplified flow diagram of a method of providing software settable access privileges within Windows NT®." Ex. 1001, 8:57–59. Patent Owner cites to the following description of Figure 6:

> In exemplary step 608, upon mounting the storage medium, ***the data relating to access privileges for the storage medium may***

> ***be loaded into the trap layer 304***. The trap layer 304 may limit operations performed on the storage medium to those supported by the read/write device by limiting the requests passed onto the file system layer 310 or, when the trap layer 304 forms part of the file system layer 310, by filtering and/or modifying the requests. ***The data relating to access privileges for the storage medium*** may be used to limit those requests provided to the file system layer 310.

See, e.g., PO Resp. 19 (citing Ex. 1001, 15:64–16:7 (emphasis added in PO Resp.)). Patent Owner contends that this passage "clearly establishes that the storage medium has associated operation access privileges—independent of the computer mounting the storage medium." *Id.*

Patent Owner, however, has not sufficiently explained how the cited passage supports its proposed claim construction of the associating step as the cited passage does not equate "associating" with either "storing" or "maintaining." Indeed, the term "associating" is not recited in this paragraph.

Furthermore, the cited passage of the '243 patent specification relates to a preferred embodiment of the invention. *See* Ex. 1001, 15:54–56 (stating Fig. 6 depicts "an exemplary method of providing software settable access privileges within Windows NR®"). It is improper to read limitations from preferred embodiments described in the specification into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited. *See Superguide Corp. v. DirecTV Enterprises, In*c., 358 F.3d 870, 875 (Fed. Cir. 2004) (stating "a particular embodiment appearing in the written description may not be read into a claim when the claim language is broader than the embodiment").

Patent Owner argues the cited portion of the specification should limit the claims because there is no other disclosure in the intrinsic record for the

association between the access privilege and medium. PO Sur-reply 4–56; *see also* Tr. 32:6–12 (stating "the purpose of the invention is to have a persistent association of . . . operation access privileges . . . with a particular storage medium. And that is the only embodiment of association that's depicted in the patent."). We disagree with this argument because the passage does not indicate that the disclosed exemplary method is the only method for providing access privileges to the system. *See* Ex. 1001, 15:54–56 (stating that Figure 6 is only "an exemplary method of providing software settable access privileges within Windows NR®").

For these reasons, we do not agree with Patent Owner that "associating, by the at least one computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium" requires that "the storage medium itself maintains its associated operation access privileges—independent of the computer" or that "the storage medium has associated operation access privileges—independent of the computer mounting the storage medium" or that operation access privileges are "persistent" so that they necessarily follow the medium from where they may be loaded when mounted. *See* PO Resp. 16–19; PO Sur-reply 3–6.

No further construction of this phrase is necessary to resolve the issues in dispute. *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))). To the extent we find it necessary to

address the meaning of any other claim terms, we do so in the context of our unpatentability analysis.

D. Asserted Art

1. Nagar (Ex. 1005)

Nagar is a developer's guide for the Windows NT operating system that is useful to those who design or implement "kernel-mode software, such as file system or device drivers." Ex. 1005, 12.[13] 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; Exs. 1001, 1004, 1015, 1016, 1018–1020); *see also* Inst. Dec. 8–9 (determining that Petitioner sufficiently established Nagar qualifies as a printed publication for purposes of institution). 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).

Nagar states that 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)." Ex. 1005, 51. "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." *Id.* Nagar states that someone who wanted to design software that could encrypt user data before the data is stored on a disk and decrypt the data before it is given back to the user could do so by designing a filter driver. *Id.* at 52. Such a filter driver that intercepts requests *above*

[13] Exhibit 1005 includes original page numbers and sequential exhibit page numbers added by Petitioner. This Decision refers to the sequential exhibit page numbers.

the file system would allow the "code to intercept the user request before the file system driver ever gets the opportunity to see it." *Id.* A filter driver that intercepts request *below the file system* would allow the driver to perform any required processing after the file system has finished its task but before the request is received by a disk driver. *Id.* Nagar Figure 2-6, reproduced below, illustrates two places where such filter driver software could be inserted. *Id*.

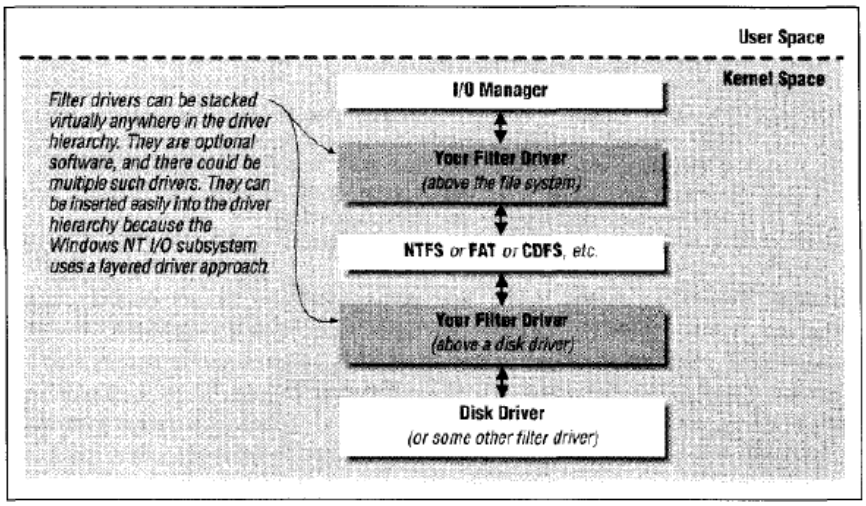

Figure 2-6. Filter drivers in the driver hierarchy

Figure 2-6 above shows that filter drivers can be "stacked virtually anywhere in the driver hierarchy" and that they can be "inserted easily into the driver hierarchy because the Windows NT I/O system uses a layered driver approach." *Id.* at 53.

Nagar also states that filter drivers can be used to "provide virus detection functionality." *Id.* at 498–499. The filter driver can have a "virus-detection module" that intercepts I/O requests before they reach the file system. *Id.* at 499. The virus-detection module can check for any virus signatures in the data being written out to the disk. *Id.* Read requests can be immediately forwarded from the filter driver to the file system. With respect

to a write request, if a virus signature is detected, the filter driver can reject the write request. *Id.* If no virus signature is detected, however, the filter driver can safely forward the I/O Request Packet ("IRP") to the file system for further processing. *Id.*

Figure 12-2 of Nagar, reproduced below, "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." *Id.* at 498.

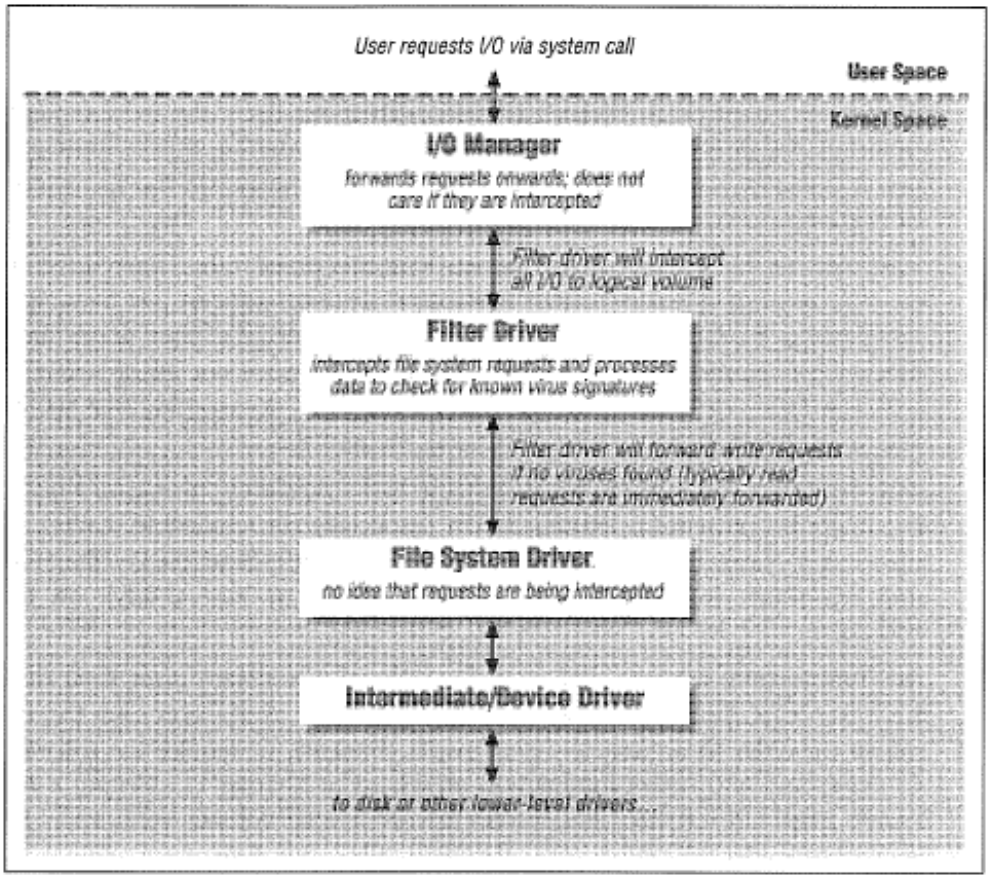

Figure 12-2. Filter driver used in virus detection

Figure 12-2 above illustrates a filter driver inserted as a layer between the I/O Manager layer and the File System Driver, wherein the filter driver

intercepts file system requests and processes data to check for known virus signatures. *See id.* at 498–499.

2. Kung (Ex. 1008)

Kung is a U.S. Patent titled "Secure File Erasure" directed to "methods of deleting (erasing) files stored on permanent storage media of a computer system that eliminates the possibility of recovery of the data as a readable file by unauthorized persons." Ex. 1008, 1:6–10. Kung discloses known techniques for such a secure erasure in which 0's and 1's are overwritten on the data to be erased. *Id.* at 1:24–29. Kung also discloses a technique of encrypting all data to be deleted so that the erased data is unreadable even if recovered. *Id.* at 3:18–62.

3. McGovern (Ex. 1006)

McGovern is a U.S. Patent Application Publication titled "System and method for record retention date in a write once read many [WORM] storage system" and describes a WORM system that stores files with a "specified retention date" to protect them "against deletion or modification." Ex. 1006, codes (54), (57), ¶ 20. Setting the retention date causes the system to observe "WORM properties" (no deletion, no modification, etc.) for the WORM file "during the applicable retention period." *Id.* ¶ 119. "[A]fter expiration of the period," the system "allows the user to perform a limited set of non-WORM actions on the now-expired WORM file," such as deletion. *Id*

4. Vossen (Ex. 1007)

Vossen is a U.S. Patent titled "Process restriction within file system hierarchies" and describes "a method and apparatus for 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. 1007, codes (54), (57). Vossen teaches "modify[ing] the usual operation of the host computer's operating system interface such that any file system access attempts by the affected process are constrained to occur logically within the restriction domain." *Id.* at 2:27–30. Vossen teaches that Windows NT supports external devices via loadable device drivers and that the operating system kernel delivers one of a large set of requests to the driver in a I/O Request Packet (or IRP) when a process requests some service of the device. *Id.* at 4:24–30.

Vossen further teaches that it is possible to add layers above file system drivers called intermediate drivers. *Id.* at 4:57–58. An intermediate driver is "known as a file system filter driver since its usual task is to filter the requests delivered to the underlying file system driver." *Id.* at 4:58–61. "A filter driver will typically examine the IRP provided by the kernel and make modifications (according to the function of the specific driver) before passing it along to the actual file system driver." *Id.* at 4:61–64. Vossen further discloses that one example of such a filter driver is a process restriction filter driver, such as that shown below in Vossen Figure 6. *Id.* at 4:64–67.

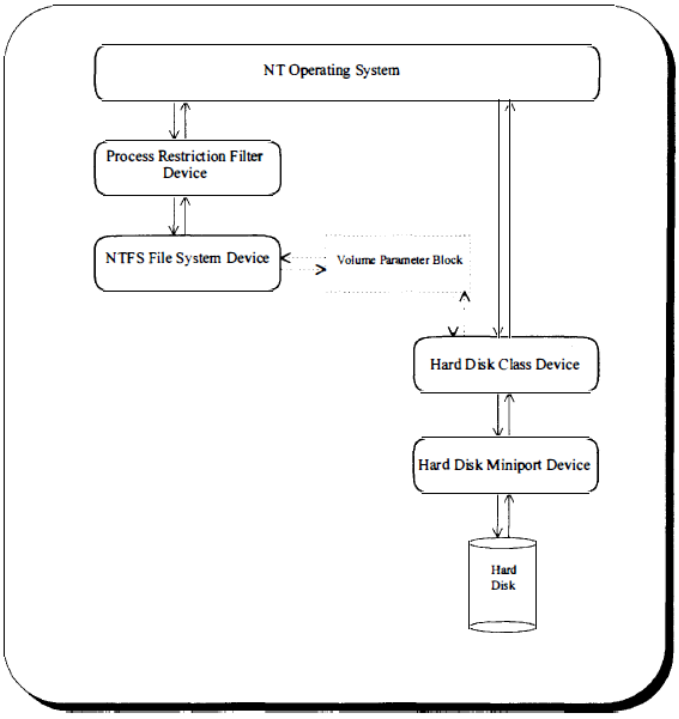

Figure 6

Figure 6 of Vossen, above, depicts an NT system configuration including a process restriction filter driver. *Id.* at 2:59–60. "[T]he process restriction filter operates by examining all IRPs containing path names sent to each file system it restricts." *Id.* at 9:65–67. "For each IRP received, the filter driver determines if the process that initiated the I/O request should be subject to file system restrictions." *Id.* at 10:6–8. The process restriction filter modifies restricted IRPs before passing them to the driver that resides below it. *Id.* at 11:1–3.

5. Denning (Ex. 1013)

Denning is non-patent literature (a book) intended for graduate level computer science courses concerning cryptography and data security.

Ex. 1013, 5–6.[14] Petitioner argues that Denning was published in 1982, and therefore qualifies as prior art under at least 35 U.S.C. § 102(b). IPR608-Pet. 11–13 (citing Ex. 1014 ¶¶ 11–13, 20–24: Exs. 1017, 1023); *see also* IPR608-Inst. Dec. 8–9 (preliminarily determining that Petitioner sufficiently established Denning qualifies as a printed publication for purposes of institution). Patent Owner does not challenge the prior art status of Denning. *See generally* PO Resp. We are persuaded that Petitioner has shown that Denning qualifies as prior art under 35 U.S.C. § 102(b).

Chapter 4 of Denning deals with access controls and, in particular, teaches that "[b]y regulating the reading, changing, and deletion of data and programs, access controls protect against accidental and malicious threats to secrecy, authenticity, and system availability." Ex. 1013, 69. Denning further teaches the importance of proper user identification and of protecting "[the] information specifying the access rights of each user or program . . . from unauthorized modification." *Id.* Denning additionally notes the difference between "policy and mechanism," explaining that "[a]n access control policy specifies the authorized accesses of a system; an access control mechanism implements or enforces the policy." *Id.* (emphases omitted).

E. Independent Claims 1, 62, and 66 – Nagar

Petitioner asserts independent claims 1, 62, and 66 of the '243 patent are unpatentable under 35 U.S.C. §§ 102, 103(a) over the teachings of

[14] Exhibit 1013 includes the original page numbers of Denning as well as sequential exhibit page numbers added by Petitioner in a footer of each page. This Decision refers to the sequential exhibit page numbers added to Exhibit 1013.

Nagar. *See* Pet. 16–22, 49–52; IPR6008-Pet. 19–35.[15] Patent Owner opposes. *See* PO Resp. 16–20. For the reasons set forth below, we determine Petitioner has shown by a preponderance that claims 1, 62, and 66 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

1. Independent Claim 1

a) Preamble and claim element 1[b]

The preamble (claim element 1[a]) and claim element 1[b] recite:

> 1. [a] A computer implemented method for applying, by at least one computer processor, a computer file system operation access privilege to a computer storage medium, comprises:
>
> [b] associating, by the at least one computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium;

Ex. 3002, 1.

Petitioner contends Nagar's disclosure of a "virus-detecting filter driver" for the Windows NT operating system that distinguishes between different types of access operations such as "read" or "write" I/O requests (computer file access privileges) acting on logical volumes (a computer storage medium) teaches the method of claim 1. Pet. 16–17 (citing Ex. 1005, 21, 40, 498–499; Ex. 1002 ¶¶ 47–48). Petitioner explains that when the operation is a "write" request, Nagar's filter driver checks for viruses (i.e., "attempts to detect viruses in the request") and rejects the write request if a virus is found as "operations containing viruses do not have

[15] Petitioner presents the same Nagar based anticipation and obviousness arguments in both IPR2019-00607 and IPR2019-00608. *See* IPR2019-00608, 19 n.3. Although this Decision cites to the parties' arguments set forth in IPR2019-00607, similar arguments were made in IPR2019-00608. *See* IPR608-Pet. 19–35; IPR608-PO Resp.16–19; IPR608-Reply 1–9; IPR608-PO Sur-reply 1–10.

writing privileges to the volume." *Id.* (citing Ex. 1005, 499). If the request is free of virus signatures, however, the filter driver forwards the request to the file system. *Id.* (citing Ex. 1005, 499; Ex. 1002 ¶ 48). Petitioner further contends that Nagar's virus-detecting filter driver, which comprises the operation access privilege, associates the claimed access privilege to the computer storage medium by attaching itself to the logical volumes (computer storage medium), satisfying the limitations of claim element 1[b]. Pet. 17–18 (citing Ex. 1005, 159).

Patent Owner makes a number of arguments as to why Nagar does not disclose all of the recitations in claim elements 1[a] and [b].

"Associating" the Access Privilege with a Portion of the Storage Medium

First, Patent Owner contends Nagar does not teach the "associating" step of claim element 1[b] because the associating step requires the storage medium itself to maintain its associated operation access privileges—independent of the computer. *See* PO Resp. 16–19; PO Sur-reply 3–10. Patent Owner argues that if Nagar's logical storage medium were dismounted or mounted on a different NT system that did not have the virus-checking software, the logical storage medium would not be subject to virus checking as the virus checking permissions are always only associated with the computer and not the medium itself. PO Resp. 18 (citing Ex. 1005, 498–499; Ex. 1002 ¶ 42).

This argument is not persuasive as it is based upon a construction of "associating" that we do not adopt. As explained in Section II.C.1 above, we do not agree with Patent Owner that "associating, by the at least one computer processor, the computer file system operation access privilege with at least a portion of the computer storage medium" recited in claim 1

requires that "the storage medium itself maintains its associated operation access privileges—independent of the computer" or that "the storage medium has associated operation access privileges—independent of the computer mounting the storage medium" or that operation access privileges are "persistent" so that they necessarily follow the medium from where they may be loaded when mounted.

We agree with Petitioner that Nagar teaches *associating an operation access privilege with at least a portion of the storage medium* by teaching that Nagar's virus-checking filter driver, which checks for read/write requests (i.e., operation access privileges), layers, or attaches, itself to the device object representing the mounted logical volume (the storage medium). *See* Pet. 16–18 (citing Ex. 1005, 159, 498–499, 506; Ex. 1002 ¶¶ 47–48). 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. 1005, 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. 1005, 159 (emphasis added).

Operation Access Privilege

Patent Owner also argues Nagar does not teach the claimed "operation access privilege" because Nagar's read and write 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 are not based on the attempted operation (*operation-based* access privileges). *See* PO

Sur-reply 1–3 (citing PO Resp. 17–19).[16] In particular, Patent Owner contends that Nagar's virus-detection software checks the content of both read and write operations for viruses and allows or denies those operations based on the presence or absence of a virus. *Id.* at 2. Patent Owner contends that, in contrast, the '243 patent applies "the operation access to the storage medium itself" by "considering whether the storage medium supports the operation at issue." *Id.* at 3 (citing Ex. 1001, 5:12–6:37).

We disagree with Patent Owner. The '243 patent states that exemplary "operation access privileges" include: "*read, write*, execute, move, rename, append, change permissions, change attributes, overwrite and/or overwrite zero length." Ex. 1001, 4:63–67 (emphasis added); *see also id.* at 4:54–56 (stating in an "exemplary aspect of the invention, the method may include where the operation access privilege is a read-only for the logical storage medium"). Petitioner argues, and we agree that Nagar expressly discloses two operation access privileges identified in the '243 patent—read and write. Ex. 1005, 498–499.

Mounted Logical Volume

Patent Owner argues that Nagar does not teach associating an operation access privilege with a storage medium because Nagar's virus-detecting filter driver "has to create a device object that layers (or attaches) itself to the device object *representing* the mounted logical volume" and

[16] Although Patent Owner cites to pages 17–19 of its Patent Owner Response for this argument, these pages of the Response relate to Patent Owner's argument that the '243 patent requires the storage medium itself to maintain the access privileges independent of the computer and not to an argument that Nagar's access privileges are not operation based access privileges.

therefore "the device object is only a representation of a mounted logical volume and not the actual storage medium itself." PO Resp. 19 n.1 (quoting Ex. 1005, 499; citing Ex. 2001 ¶ 44). Patent Owner contends that a person of ordinary skill in the art "would not understand a representation of a mounted logical volume (portion of a storage medium) to be the same as the actual storage medium." *Id.* (citing Ex. 2001 ¶ 44).

We disagree with Patent Owner's argument because the claims require "*associating* . . . the computer file system operation access privilege with . . . a portion of the computer storage medium" and do not require that the access privileges be stored on the computer storage medium itself. *See supra* Section II.C.1. We agree with Petitioner's assertion that "associating with a computer storage medium is achieved by attaching to a device object, because a computer views the storage medium as a device object." Reply 8 (citing Ex. 1005, 155–156). 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. 1005, 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." *Id.* at 156. Dr. Weissman persuasively explains that a person skilled in the art would have appreciated that the privileges for operations on a file or directory—a portion of the storage medium—are associated with those target file/directory objects. *See* Ex. 1002 ¶ 174; *see also* Reply 8.

Additionally, the '243 patent states that "a storage medium [is] within the file system layer 310 of the system" thus indicating that an actual storage medium is managed via its logical representation in the file system. *See*

Ex. 1001, 15:31–32; Reply 8. Thus, we agree with Petitioner's assertion that "associating with a computer storage medium is achieved by attaching to a device object, because a computer views the storage medium as a device object." Reply 8 (citing Ex. 1005, 155–156).

In its Sur-reply, Patent Owner also argues that Petitioner's reliance on a *logical* storage medium in Nagar fails because the claim recites a "storage medium" and a logical storage medium is not a storage medium. *See* PO Sur-reply 7–10; *see also id.* at 9 (stating independent claims 1, 62, and 66 do not "associate operation access privileges with a 'logical' storage medium, but instead with a 'storage medium'"). The '243 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, 4:26–28. Thus, the specification of the '243 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. As such, 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.

b) Remaining Undisputed Subject Matter of Claim 1

Petitioner asserts Nagar discloses the remaining limitations of claim 1. *See* Pet. 16–22. Other than the arguments already discussed above, Patent Owner does not separately argue the patentability of claim 1 based on these remaining limitations. *See generally* PO Resp.; PO Sur-reply. We have reviewed Petitioner's argument and evidence and agree that Nagar discloses the remaining limitations of claim 1.

For example, Petitioner asserts, and we agree, that Nagar's disclosure of a filter driver that intercepts all I/O requests to the logical volume

discloses the intercepting step of claim element 1[c], which recites "intercepting . . . by at least one computer file system trap layer or at least one file system filter layer, an attempted operation on said at least a portion of the computer storage medium." Pet. 18–19 (citing Ex. 1005, 496, 498–499, Fig. 12-2; Ex. 1002 ¶¶ 50–51); Ex. 3001, 1. Petitioner also asserts, and we agree, that Nagar discloses "wherein said intercepting occurs regardless of an identity of a user attempting the attempted operation" recited in claim element 1[d] because Nagar discloses intercepting all I/O requests, including read and write requests, without regard to the identify of a user attempting a particular operation. Pet. 20 (citing Ex. 1005, 18, 134, 195, 498–499; Ex. 1002 ¶¶ 52–56).

Petitioner also asserts, and we agree, that Nagar discloses the comparing step of claim element 1[e] ("comparing, by the at least one computer processor, the attempted operation to the computer file system operation access privilege") and the allowing or denying step of claim element [f] ("allowing, or denying, by the at least one computer processor, the attempted operation based on the comparing the attempted operation to the computer file system operation access privilege") by disclosing that the filter driver checks the access privileges associated with the I/O requests (i.e., a read or write request) and (1) in the case of a read request, allows the operation (by forwarding the request to the file system driver), and (2) in the case of a write request, checks for viruses and either allows the write if no virus is detected or rejects the write if a virus is detected. *See* Pet. 20–22 (citing Ex. 1009, 498–499; Ex. 1002 ¶¶ 57–59).

c) Conclusion

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 '243 patent is unpatentable under 35 U.S.C. §§ 102, 103 over Nagar. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1373 (Fed. Cir. 2019) ("[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.'").

2. Independent Claims 62 and 66

Petitioner asserts claims 62 and 66 are substantially similar to claim 1 and that Nagar anticipates or renders obvious claims 62 and 66 for the same reasons set forth with respect to claim 1. Pet. 49–51, 51–52; Ex. 1001, 46:14–16, 46:63–67; Ex. 3002. Patent Owner relies on the same arguments for claims 62 or 66 as it does for claim 1. *See* PO Resp. 16. We have reviewed Petitioner's argument and evidence and determine that Petitioner has sufficiently shown that Nagar discloses or suggests the recitations of 62 and 66.

For example, the preamble of claim 62 recites a "non-transistory computer accessible storage medium embodied thereon computer program product, said computer program product for applying a computer file system operation access privilege to a computer storage medium when executed on at least one computer processor, performing a method of." Ex. 1001, 46:7–13. The preamble of claim 66 recites a "data processing system configured to apply a computer file system operation access privilege to a computer storage medium, comprises." *Id.* at 46:60–63.

Petitioner contends, and we agree, that Nagar teaches these preambles for the same reasons Nagar discloses the preamble of claim 1.[17] *See* Pet. 49, 51. Petitioner persuasively explains that a POSITA would have understood that Nagar's virus-detecting filter driver, which is described as a "software module," is a "'computer program product' that would be embodied on a 'non-transitory computer accessible storage medium'" as recited in the preamble of claim 62. *See id.* at 49–50 (emphases omitted) (citing Ex. 1005, 51, 134–135, 497–499, Ex. 1002 ¶¶ 117–118). Petitioner also asserts that a POSITA would have understood that Nagar's methods are computer implemented by one or more computer processors in a data processing system containing a computer storage medium, and are applicable to computer file systems, as recited in the preamble of claim 66. *Id.* at 51 (citing Ex. 1002 ¶ 130).

We agree with Petitioner that the remaining elements of claims 62 and 66, which are similar to elements recited in claim 1, are taught by Nagar for the same reasons set forth in connection with claim 1. *See* Pet. 50–52.

Thus, Petitioner has shown by a preponderance of the evidence that independent claims 62 and 66 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

F. Claims 2, 3, 63, 67, and 68 – Nagar

Petitioner asserts dependent claims 2, 3, 63, 67, and 68 of the '243 patent are unpatentable under 35 U.S.C. §§ 102, 103(a) over the teachings of Nagar. *See* Pet. 22–26, 51–52; Reply 9–11. Patent Owner opposes. *See* PO

[17] We do not reach the issue of whether the preambles of claims 62 and 66 are limiting as we are persuaded by Petitioner's arguments that the recitations in the preambles are satisfied by the prior art.

Resp. 20–21; PO Sur-reply 11–13. For the reasons set forth below, we determine Petitioner has shown by a preponderance that claims 2, 3, 63, 67, and 68 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

1. Claims 2, 63, 67

Claim 2 recites:

> 2. The method according to claim 1 wherein said allowing or denying, by the at least one computer processor, comprises at least one of:
>
> [a] allowing, or denying, by the at least one computer processor, the attempted operation based on a content of a logical file associated with said at a least a portion of the computer storage medium.

Ex. 1001, 32:1–7 (bracketed material and formatting added for clarity); Ex. 3002, 1.

Claim 63 recites:

> 63. The computer program product according to claim 62, wherein said allowing or said denying of the attempted operation of the method comprises at least one of:
>
> [a] allowing, or denying, by the at least one computer processor, the attempted operation based on a content of a logical file associated with said at least a portion of the computer storage medium;
>
> [b] allowing, or cancelling, by the at least one computer processor, the attempted operation based on the content of the file; or
>
> [c] allowing, by the at least one computer processor, a create file operation to create a file on at least a portion of the computer storage medium, evaluating, by the at least one computer processor, a content of the file, and at least one of:

> allowing, by the at least one computer processor, the attempted operation, or
>
> deleting, by the at least one computer processor, the file based on said evaluating.

See Ex. 1001, 46:31–48 (bracketed material and formatting added for clarity). Claim 67 recites similar subject matter similar to limitations recited by claim element 63[a]. *See* Ex. 1001, 47:13–18.

Petitioner contends Nagar discloses the limitations of claims 2, 63, and 67 because Nagar discloses allowing/denying a write request (the attempted operation) based on a virus evaluation of a file to be copied to (i.e., associated with) a mounted logical volume. *See* Pet. 22–25, 51–52; Ex. 1002 ¶¶ 61–63; Reply 9–10. Petitioner asserts that both (1) the virus signatures for the filter driver and (2) the data in the files that are being copied and mounted onto the logical volume are "content of a logical file associated with said at least a portion of the computer storage medium." Pet. 23 (citing Ex. 1005, 498-499; Ex. 1002 ¶ 61). Petitioner contends that the virus signatures for the filter driver are content of a logical file associated with the storage medium because the filter driver is a logical file and the virus signatures are organized data (content) of the filter driver (logical file). Petitioner further contends that Nagar's filter drivers are associated with the storage medium because Nagar teaches that the "filter driver 'layers (or attaches) itself to,' i.e., is *associated with*, 'the device object representing the mounted logical volume.'" *Id*. (citing Ex. 1005, 159, 499); *see also id.* (stating Ex. 1005, 159 describes "how filter drivers attach themselves to logical volumes").

Petitioner also asserts that files being copied to the mounted logical volume are logical files and that the files are *associated* with storage

medium because they are being copied to the storage medium. *See id*. at 23–24 (citing Ex. 1005, 498; Ex. 1002 ¶ 63).

In response, Patent Owner contends that because Nagar does not write the content of a file onto the storage medium until *after* it determines the file does not contain a virus, Nagar does not teach allowing an operation based on the content of a logical file associated with the storage medium. *See* PO Resp. 20–21 (citing Ex. 2001 ¶ 47); s*ee also id.* at 20 (stating "[b]ecause Nagar does not create a file on the computer storage medium without at least first evaluating the content, even if such content were in a logical file not on the storage medium, there is no 'content of a logical file ***associated with*** said at least a portion of the computer storage medium' because there is nothing written in Nagar onto the storage medium unless no virus signature is detected"). Thus, Patent Owner contends there must be a file created on or written onto the storage medium for there to be a logical file "associated with" the storage medium.

For the following reasons, we are not persuaded by Patent Owner's argument, and we determine Nagar discloses the limitations of claims 2, 63, and 67.

First, Patent Owner's arguments do not address why the virus signatures of the filter driver that are attached to the storage medium are not logical files associated with the storage medium. As asserted by Petitioner, we determine that Nagar teaches allowing or denying an operation based on evaluating the virus signatures.

Second, we disagree with Patent Owner's contention that the logical file must be created on or written onto on the storage medium in order for the file to be "associated" with the storage medium. *See* PO Resp. 20–21;

Sur-reply 11. As explained *supra* in § II.C.1, in connection with the phrase of claim element 1[b] which requires *associating* an operation access privilege with the storage medium, the plain meaning of the term "associating" with does not require "written on" or created on. Similarly, a logical file need not be *created on* or *written onto* a storage medium in order to be *associated with* a storage medium. We are persuaded by Dr. Weissman's testimony that a file that is being copied to a mounted logical volume is a "logical file associated with said at least a portion of the computer storage medium." Ex. 1002 ¶¶ 61–63 (citing Ex. 1005, 498–499); Pet. 23–24. Thus, Petitioner has persuasively shown that the file that is to be written to the storage medium is associated with the storage medium.

We also agree that Nagar teaches allowing, or denying, by the at least one computer processor, the attempted operation based on a content of a logical file associated with said at least a portion of the computer storage medium as recited in claim element 2[a], 63[a], and similarly recited in claim 67. Pet. 22–25 (citing Ex. 1002 ¶¶ 61–63; Ex. 1005, 498, Fig. 12-2). Petitioner persuasively shows that Nagar teaches allowing or denying a write request (attempted operation) based on the content of the logical file (the content of either the filter driver or the content of file being copied to the storage medium) by allowing or denying the request based on whether it has a viral signature. *Id.* at 24–25; *see also* Ex. 1001, 18:65–19:5 (stating that in an exemplary embodiment, the trap layer determines if an operation is eligible to be executed on a file based on the content of the file and may determine that a file is harmful if the file is a "computer virus, malware" and may prevent harmful files from being created). Thus, Petitioner has shown Nagar anticipates claims 2, 63, and 67.

Patent Owner also contends that Nagar's failure to teach creating a file that is associated with the storage medium is "even more glaring in the context of claim 63, which provides for a 'create file operation' in the case where there is no file already associated with the storage medium the content of which to evaluate." PO Sur-reply 13.

We disagree that this argument shows that claim 63 is patentable. The "create file" operation is only found in claim element 63[c], which is one of the Markush groups recited in claim elements 63[a]–[c]. As noted above, Petitioner has shown that Nagar teaches the limitations of claim element 63[a].

Thus, Petitioner has shown by a preponderance of the evidence that claims 2, 63, and 67 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

2. Claims 3 and 68

Claim 3 depends from claim 2 and further recites:

> wherein said allowing, or said denying, by the at least one computer processor, comprises at least one of: allowing, or cancelling, by the at least one computer processor, the attempted operation based on the content of the file.

Ex. 1001, 32:8–13; Ex. 3002, 1. Claim 68 recites similar limitations. *See* Ex. 1001, 47:19–22. Petitioner contends Nagar discloses the limitations of claims 3 and 68 for the same reasons Nagar discloses allowing the attempted operation based on the content of a logical file as recited in claim 2, namely because Nagar discloses "allowing" an attempted write request if it does not detect a virus signature in the data that is being copied to the logical volume. Pet. 26, 52 (citing Pet. 22–25; Ex. 1002 ¶ 65). Patent Owner does not

separately address Petitioner's contentions as to claims 3 and 68. *See generally* PO Resp.

We are persuaded by Petitioner's contentions and evidence that Nagar discloses the limitations of claims 3 and 68, and we determine that Petitioner has proven by a preponderance of the evidence that claims 3 and 68 of the '234 patent are unpatentable under 35 U.S.C. §§ 102 and 103(a) over Nagar.

G. Claims 4, 34, 69 and 103 – Nagar

Petitioner asserts dependent claims 4, 34, 69 and 103 of the '243 patent are unpatentable under 35 U.S.C. §§ 102, 103(a) over the teachings of Nagar. *See* Pet. 26–28, 51–52; Reply 11–14. Patent Owner opposes. *See* PO Resp. 21–24; PO Sur-reply 13–15. For the reasons set forth below, we determine Petitioner has not shown by a preponderance that claims 4, 34, 69 and 103 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

Claim 4 depends from claim 1 and further recites:

> [a] wherein said allowing, or said denying, by the at least one computer processor, the attempted operation comprises:
>
> [b] allowing, by the at least one computer processor, a create file operation to create a file on at least a portion of the computer storage medium;
>
> [c] evaluating, by the at least one computer processor, a content of the file; and
>
> [d] at least one of:
>
> allowing, by the at least one computer processor, the attempted operation, or
>
> deleting, by the at least one computer processor, the file based on said evaluating.

Ex. 1001, 32:18–27; Ex. 3002, 2 (brackets and formatting added for clarity). Dependent claims 34, 69, and 103 each recite similar limitations.[18] *See id.* at 41:46–49, 47:26–30, 54:54–57.

Petitioner contends Nagar teaches these elements by teaching allowing a write request for copying data or files (an attempted operation) to a mounted logical volume (computer storage medium). *See, e.g.,* Pet. 26–27 (citing Ex. 1005, 498); Ex. 1002 ¶ 67. Petitioner further contends that Nagar's write request allows a "create file operation" as recited in claim element 4[b] because a file must be created in order to perform the write operation. *See* Pet. 27 (citing Ex. 1005, 39, 552; Ex. 1002 ¶ 67). Petitioner further asserts Nagar teaches the evaluating step of claim element 4[c] by checking whether the content of the file attempted to be written to the mounted logical volume contains a computer virus. *Id.* (citing Ex. 1002 ¶ 68). Petitioner also contends that Nagar teaches the allowing limitations of claim element 4[d] by allowing the attempted write operation if the data attempted to be written into the file on the logical volume does not contain any computer virus. *Id.* at 28 (citing Ex. 1002 ¶ 69).

Patent Owner responds that Nagar does not disclose the steps of claim 4 in the order required by the claim because Nagar does not first create a file on the storage medium as required by claim element 4[b] and then *evaluate* "the content of the *created file*" as required by step 4[c]] and then

[18] Patent Owner asserts that claim 63 also includes limitations similar to claim 4. PO Resp. 21. However, as discussed above, the relevant feature of a "create file" operation is one of the Markush groups recited in claim 63 which does not need to be performed to meet the limitations of the claim. Having determined that claim 63 is unpatentable for the same reasons as claim 2, we do not address claim 63 here.

either allow the attempted operation or delete the file as required by step 4[d]. *See* PO Resp. 21–23 (citing Ex. 2001 ¶ 50); *see also id.* at 22 (stating the "the allowing the attempted operation or deleting the file is based on the evaluating of *the content of the created file*") (emphasis altered). Patent Owner contends that because Nagar evaluates the content of the file *before* allowing the writing of the file to the computer storage medium (i.e. allowing the attempted operation), Nagar does not disclose allowing the attempted operation (step 4[d]) based on evaluating content of the file that has already been created on the computer storage medium (step 4[c]). *Id.* at 22–23 (citing Pet. 28; Ex. 2001 ¶¶ 50–51; Ex. 1005, 49). Patent Owner further argues Nagar does not teach the similar limitations recited in claims 34, 69 and 103. PO Resp. 21.

We agree with Patent Owner. The antecedent basis for "the file" recited in claim element 4[c] is "a file on at least a portion of the storage medium" as recited in claim element 4[b]. Thus, claim 4[c] requires "evaluating . . . a content of the file" that is "on at least a portion of the storage medium." Petitioner argues that, in Nagar, the filter driver "evaluates any data content *attempted to be written* to the file and allows the attempted write operation if no virus is found in the data." Reply 14 (citing Ex. 1005, 498; Pet. 26–28, 34–35) (emphasis added). However, because Nagar's evaluation occurs on the data *attempted to be* written to the file on the storage medium, the data that is evaluated is not "content of the file" that is on the storage medium.

Petitioner also argues that a person skilled in the art would have found it desirable to create a placeholder file without content before the write request is allowed. *See* Pet. 58–61; Reply 11 (citing Ex. 1005, 497). This

argument is not persuasive because, even if a person skilled in the art would have created a placeholder file on the storage medium before the write request is allowed, the placeholder file would not contain any content until *after* the filter driver determines that the evaluated data is virus free. Thus, Nagar does not teach evaluating content of a file *on a* computer storage medium as required by claim 4.

For the foregoing reasons, Petitioner has not sufficiently shown that Nagar discloses or suggests all of the limitations of claim 4, or the limitations similarly recited in claims 34, 69 and 103. Therefore, Petitioner has not shown by a preponderance of the evidence that claims 4, 34, 69 and 103 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

H. Claims 32, 61, 101 – Nagar

Petitioner asserts dependent claims 32, 61, and 101 of the '243 patent are unpatentable under 35 U.S.C. §§ 102, 103(a) over the teachings of Nagar. *See* Pet. 31–33, 48–49, 52; Reply 14–17. Patent Owner opposes. *See* PO Resp. 24–27; PO Sur-reply 15–18. For the reasons set forth below, we determine Petitioner has shown by a preponderance that claims 32, 61, and 101 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

Claim 32, which depends from claim 1, and claim 101, which depends from claim 66, each recite "wherein said at least one computer file system trap layer or said at least one computer file system filter layer is implemented within a file system layer." Ex. 1001, 41:34–36, 54:42–45. Dependent claim 61 recites a similar element. *Id.* at 46:5–6.

Relying on annotated Figure 2-6 of Nagar, Petitioner contends Nagar discloses implementing a computer file system trap layer (filter driver) within a file system layer (annotated box below labeled "File System Layer"

containing both the file system and disk driver) by teaching that the filter driver can be stacked anywhere in the driver hierarchy, including below the NTFS/FAT/CDFS layer and above the disk driver. *See* Pet 31–33 (citing Ex. 1005, 53, 134, Fig. 2-6; Ex. 1002 ¶¶ 73–77).- Figure 2-6 of Nagar, with annotations provided by Petitioner, is reproduced below.

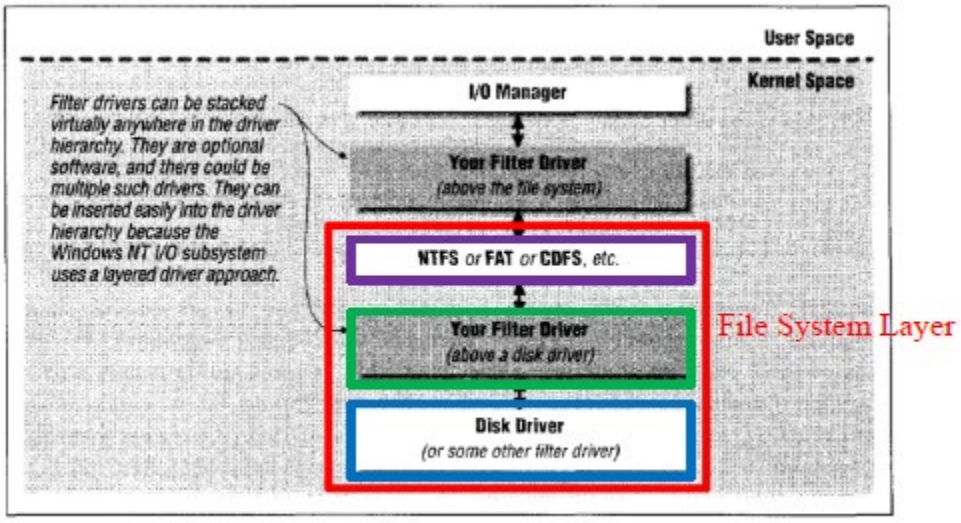

Figure 2-6. Filter drivers in the driver hierarchy

Figure 2-6 of Nagar, with color annotations by Petitioner, illustrates that "[f]ilter drivers can be stacked virtually anywhere in the driver hierarchy." Ex. 1005, 53.

Patent Owner contends that because Nagar's "file system layer" corresponds to the NTFS/FAT/CDFS layer shown in Nagar's Figure 2-6, and because Nagar's filter driver is inserted either above or below, but not "within" the NTFS/FAT/CDFS layer, Nagar does not teach inserting its filter driver *within* the file system layer of Windows NT. PO Resp. 24–27 (citing Ex. 1005, 51, 53, Fig. 2–6; Ex. 2001 ¶¶ 54–57); PO Sur-reply 15–18 (citing Ex. 1001, 13:36–42; 15:31–32 & 61-63; 15:27–16:8, Fig. 6; Ex. 1005, 51–53; Ex. 2001 ¶¶ 54–57). Patent Owner further contends that the '243 patent "discloses that its file system trap layer 'which may also be referred to as a

filter layer' cannot be implemented within the file system layer of Windows NT but can be implemented within the file system layer of other operating systems/file systems." PO Resp. 24–27 (citing, *inter alia*, Ex. 1001, 13:20–22, 13:36–42).

We disagree with Patent Owner's arguments and agree with Petitioner that the file system layer of the '243 patent can include a disk driver, even in a Windows NT environment.

As admitted by Patent Owner, the '243 patent describes "other environments" besides Windows NT that "may permit implementing a trap/filter layer within the file system layer." PO Resp. 27 (citing Ex. 1001, 8:60–62, 12:18–22, 13:36–42, 15:64–16:7, FIG. 7; Ex. 2001¶ 57). Patent Owner appears to contend that because the '243 patent discloses embodiments that are both related and unrelated to the Windows NT environment and (1) an exemplary embodiment within a Windows NT environment shows the trap layer outside of a file system layer and (2) alternative embodiments that are not within a Windows NT environment show a trap layer/filter layer within a file system layer, this means that the '243 patent "make[s] clear that the trap layer cannot be 'implemented within a file system layer' within windows NT." PO Resp. 25 (citing Ex. 1001, 13:36–42); *see also id.* at 26–27 (citing Ex. 1001, 8:60–62, 12:18–22, 13:36–42, 15:64–16:7, FIG. 7; Ex. 2001 ¶¶ 54–57); PO Sur-reply 16–17 (citing, *inter alia,* Ex. 1001, Figs. 5, 6). We disagree that the '243 patent's disclosure of various embodiments means that the claims are limited to any of the disclosed embodiments such that the claims would exclude a trap layer implemented within the file system layer of Windows NT but would

cover a trap layer implemented within the file system layer of other operating systems/file systems. *See* PO Resp. 24–27.

As Petitioner persuasively argues, the '243 patent explains that the "'file system layer' includes both the file system and disk driver." *See* Pet. 32 (citing Ex. 1001, 15:31–32, 15:61–63; Ex. 1002 ¶ 75). In particular, the '243 patent discloses the following: "In exemplary step 606, upon mounting the storage medium, data relating to, for example, physical limitations of the read/write device may be loaded into the device driver for that device within the file system layer 310." Ex. 1001, 15:60–63. This disclosure is in a discussion of Figure 6, which is "a simplified flow diagram of an exemplary method of providing software settable access privileges within Windows NT®." Ex. 1001, 15:54–56. Thus, in the '243 patent, the file system layer includes the file system and the disk driver, even in Windows NT. We are persuaded, therefore, by Petitioner's argument, which relies on this disclosure in the '243 patent as to the scope of "file system layer," that Nagar's disclosure of a filter driver between the file system and the disk driver, both of which are encompassed with the claimed "file system layer," describes "wherein said at least one computer file system trap layer or said at least one computer file system filter layer is implemented within a file system layer." *See* Pet. 31–32.

We also disagree with Patent Owner's argument that because (1) Nagar's "file system layer" corresponds to the NTFS/FAT/CDFS layer shown in Nagar's Figure 2-6 and (2) Nagar's filter driver is inserted either above or below, but not "within" the NTFS/FAT/CDFS layer, this means Nagar does not teach inserting its filter driver *within* the file system layer of Windows NT. *See* PO Resp. 24–27. As explained above, the scope of the

claimed "file system layer" in the '243 patent includes the file system and the disk driver. Patent Owner argues, and Dr. Melendez testifies, that a person of ordinary skill in the art would have understood the box in Nagar's Figure 2-6 labeled "**NTFS** or **FAT** or **CDFS**, *etc*." to be the file system layer. PO Resp. 26; Ex. 2001 ¶ 56. But this position fails to appreciate the scope of the claimed "file system layer" as including the file system and the disk driver, as that term is used in the '243 patent.

Thus, for the foregoing reasons, Petitioner has shown that Nagar discloses the limitations of claim 32, and the similar limitations of claims 61 and 101, which Patent Owner does not dispute separately, and therefore has shown by a preponderance of the evidence that claims 32, 61, and 101 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar.

I. Claims 24, 25, 32, 33, 35–37, 39, 54–57, 61, 87–89, 93, 94, 101, 10 – Nagar

Petitioner contends that claims 24, 25, 32, 33, 35–37, 39, 54–57, 61, 87–89, 93, 94, 101, and 102 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar. Pet. 28–49, 52–66. Patent Owner does not respond to these contentions (*see generally* PO Resp.), and, based upon a review of the complete record in each proceeding, we find that Petitioner makes a persuasive showing. *See* Paper 12 (Scheduling Order), 7 (stating "any arguments not raised in the response may be deemed waived").

We conclude that Petitioner has shown by a preponderance of the evidence that claims 24, 25, 32, 33, 35–37, 39, 54–57, 61, 87–89, 93, 94, 101, and 102 are unpatentable under 35 U.S.C. §§ 102, 103(a) over Nagar..

J. Claims 16, 26, 81, and 95 – Nagar and Kung

Petitioner asserts claims 16, 26, 81, and 95 would have been obvious over the combined teachings of Nagar and Kung. Pet. 66–73; Reply 17–23. Patent Owner opposes. PO Resp. 27–38; PO Sur-reply 18–20. For the reasons that follow, we determine claims 16, 26, 81, and 95 would have been obvious over Nagar and Kung.

1. Claims 16 and 81

Claim 16 depends from claim 1 and further recites:

> wherein said allowing, or said denying, by the at least one computer processor, the attempted operation comprises:
>
> [a] forcing, by the at least one computer processor, a secure erasure for a delete operation on said at least a portion of the computer storage medium, wherein the secure erasure comprises at least one of:
>
> [b] overwriting, by the at least one computer processor, the content of said at least a portion of the computer storage medium, or
>
> [c] overwriting, by the at least one computer processor, an alternate data stream associated with said at least a portion of the computer storage medium.

Ex. 1001, 34:44–53 (brackets and formatting added for clarity). Thus, claim 16 requires "forcing . . . a secure erasure for a delete operation" on a storage medium either by (1) "overwriting . . . the content" of the storage medium as recited in claim element 16[b] or by (2) "overwriting . . . an alternate data stream associated" with the computer storage medium as recited in claim element 16[c]. Claim 81, which depends from claim 66, recites similar limitations. *Id.* at 48:63–49:3.

Petitioner asserts Kung teaches the additional limitations of claims 16 and 81. Pet. 66, 69–70; Reply 17–21. Petitioner contends Kung teaches the "forcing" step of claim element 16[a] by teaching a method of securely deleting or erasing a file residing on a storage medium of a computer system to make the file unreadable or unrecoverable by unauthorized persons. Pet. 69 (citing Ex. 1008, code (57), 1:24–29). Petitioner asserts, *inter alia,* that the "Background" section of Kung teaches a "conventional" method of file deleting that involves overwriting 0's and 1's over an entire file and that this method teaches the "forcing . . . a secure erasure" by "overwriting . . . the content" of the storage medium limitations recited in claim elements 16[a] and [b]. Pet. 66, 69–70 (citing Ex. 1008, 1:24–29; Ex. 1002 ¶ 276); Reply 17–18, 20.

Petitioner also argues that the "Summary of the Invention" and the "Detailed Description" sections of Kung describe an encryption method that destroys or overwrites a random external key used for encrypting a deleted file. Petitioner contends that Kung's random external key is an "alternative data stream" associated with the deleted file and that overwriting the random external key teaches "forcing . . . a secure erasure" by "overwriting . . . an alternate data steam" as recited in claim elements 16[a] and [c]. *See* Pet. 66, 70 (citing Ex. 1008, 1:40–45, 3:18–62; Ex. 1002 ¶¶ 268, 277); Reply 19 (citing Ex. 1001, 3:40–45).

Petitioner further asserts a person of ordinary skill in the art would have combined Kung's secure file-erasure methods with Nagar's filter drivers to provide heightened security to Nagar's file system and that the combination applies a known technique (Kung's secure file-erasure methods) to a known method ready for improvement (Nagar's filter drivers)

to yield predictable results (enhanced security in Nagar's system). Pet. 66–69; Ex. 1002 ¶¶ 269–274. Petitioner contends claim 81 would have been obvious over Nagar and Kung for the same reasons asserted in connection with claims 66 and 16. Pet. 73; Ex. 2001 ¶ 285.

We have reviewed Petitioner's arguments and evidence and agree that Petitioner has shown that Kung discloses the limitations of claims 16 and 81 and has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and Kung. *See* Pet. 66–70, 73; Reply 17–23.

Patent Owner makes a number of arguments in response, none of which we find persuasive. *See* PO Resp. 27–33; PO Sur-reply 18–21. First, Patent Owner argues that Kung teaches away from using the conventional method of overwriting content with Nagar's system because Kung describes the conventional method as "slow" and states the invention disclosed in Kung as "eliminates the weaknesses" associated with the conventional methods. *See* PO Resp. 28 (citing Ex. 1008, 1:27–29, 1:46–52; Ex. 2001 ¶ 60).

We are not persuaded by this argument. 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. A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art, including non-preferred embodiments. 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.* 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. 66–68 (citing Ex. 1002 ¶¶ 269–274). We do not find Kung's disclosure of a drawback to this approach—slower speed—as teaching away from the benefits it teaches of secure erasure. *See Merck & Co., Inc. v. Biocraft Labs., Inc.*, 874 F.2d 804, 807 (Fed. Cir. 1989) (stating "all disclosures of the prior art, including unpreferred embodiments, must be considered").

Patent Owner also contends that because Kung's conventional method overwrites data with 0's and 1's in response to a *user* action to delete a file, Kung teaches away from the independent claims that require intercepting an attempted operation "regardless of the identity of a user." *See* PO Resp. 31–32 (citing Ex. 1008, 1:24–27); PO Sur-reply 19–20 (citing Ex. 2001 ¶ 71). We disagree. 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 (emphasis added). We are persuaded by Dr. Weissman's testimony that a POSITA would have been motivated to modify the computerized systems in Nagar to have the system use the conventional process of overwriting 0's and 1's over the entire data file to delete the contents of the file. Ex. 1002 ¶¶ 276–278; Reply 18. Thus, we are persuaded by Petitioner's contentions that Kung's disclosure of the conventional method of overwriting data with 0's and 1's teaches the limitations set forth in claim elements 16[a] and [b].

Patent Owner also contends that because Kung's encryption method permits recovery of the encrypted data, Kung's encryption method teaches away from "secure erasure" as claimed in the '243 patent because the '243 patent "claims a novel method of secure erasure where there is no possibility that a file may be readable by any person . . . consistent with, for example, the noted secure erasure requirements of the U.S. Department of Defense in DOD 5015.2." PO Resp. 28–29 (citing Ex. 1001, 25:22–28; Ex. 1008, code (57), 1:24–29, 1:64–66, 2:3–8, 2:36–40, 3:43–45, 3:50–58, 4:3–7, Fig. 1; Ex. 2001 ¶¶ 60–61). Patent Owner also contends that Petitioner's argument—that Kung's encryption method that destroys or overwrites a random external key used for encrypting a deleted file teaches the limitations of claim element 16[c]—must fail because in this method, the "data content is encrypted and not overwritten" and Kung's deleted files are recoverable by application of the correct key. *See* PO Resp. 28–33 (citing, *inter alia* Ex. 1008, 1:64–66, 2:3–8, 2:36–40, 3:43–45, 3:50–58, 4:3–7, Figure; Ex. 2001 ¶¶ 60–65); *see also id.* at 31 (stating "regardless of whether a key may be retrieved to read the file, the content remains on the storage medium and is not overwritten"); *id.* at 33 (stating destruction of Kung's encryption key does not provide "secure erasure for a delete operation") (citing Ex. 2001 ¶ 66); *see also* PO Sur-reply 19 (stating "[e]ncyption is not equivalent to deletion . . . Secure erasure is intended to destroy the data and is not reversible and is not related to the actual data").

We are not persuaded by these arguments. First, we disagree with Patent Owner that a "secure erasure" excludes encryption or that the '243 patent teaches away from using encryption to provide a secure erasure. As noted above, Patent Owner contends that the '243 patent "claims a novel

method of secure erasure where there is no possibility that a file may be readable by any person . . . consistent with, for example, the noted secure erasure requirements of the U.S. Department of Defense in DOD 5015.2." PO Resp. 28–29 (citing Ex. 1001, 25:22–28; Ex. 2001 ¶ 61). Neither the disputed claims nor the preferred embodiment discussed in the cited portion of the '243 patent state that "secure erasure" excludes encryption.

Moreover, Kung itself states that its encryption method is a "secure deletion method" that prevents any utility program from recovering any information from a deleted file and therefore, "no information can be retrieved nor derived from the encrypted, deleted file." *See* Ex. 1008, 2:9–14. Additionally, Kung explains that in its one-way deletion mode, once the "random external key" is destroyed, "the data cannot be decrypted and is thus unreadable by anyone." *Id.* at 3:34–45. Specifically, Kung explains that in its one way deletion mode, when the user does not expect to undelete the data, "the data in . . . file 20 is encrypted using . . . random external key 21, and then . . . key 21 is automatically destroyed 19 and cannot be used to recover the data. Consequently without . . . key 21, the data cannot be decrypted and is thus unreadable by anyone." Ex. 1008, 3:37–45. Thus, we disagree with Patent Owner's contention that recovery of the data is still possible after the key is destroyed internally. *See* PO Resp. 30–31. Kung expressly states that, by destroying (overwriting) the random external key, the data on the file cannot be recovered by anyone. *See* Ex. 1008, 3:37–45.

Patent Owner also contends that Kung's encryption key is not an "alternate data stream" and even if it is, its destruction does not provide "secure erasure for a delete operation." PO Resp. 33 (citing Ex. 2001 ¶ 66). We disagree. The '243 patent describes the "alternate data stream" as

including data related to attributes of a file and stored separately from the file. *See, e.g.,* Ex. 1001, 22:67–23:2 (stating "one or more alternate data streams or extended attributes to store the legal hold information about the retained file"), *id.* at 23:56–58 (stating "creating a number of alternate data streams or extended attributes to store additional information about the file"); *id*. at 24:23–24 (stating "the policy may be stored as an alternate data stream"), *id.* at 25:60–64) (stating "the trap layer may obfuscate the user data by storing it in alternate data streams or alternate locations rendering the files unreadable and even as far as inaccessible outside the context of the trap layer"). We agree with Petitioner that Kung's encryption key is an alternate data stream because, *inter alia*, it is the key for encrypting the file (i.e., related to attributes of a file) and is stored externally (i.e., stored separately from the file). *See* Reply 19 (citing Ex. 1008, 2:31–35).

Thus, we are persuaded by Petitioner's contentions that Kung's one-way encryption method teaches the limitations set forth in claim elements 16[a] and [c].

Having considered the full record developed by trial, we are persuaded by Petitioner's contentions and evidence that Kung and Nagar teach all of limitations of claims 16 and 81 and determine that Petitioner has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and Kung. Pet. 66–70, 73; Ex. 1002 ¶¶ 266–278. We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 16 and 81 would have been obvious over the combination of Nagar and Kung.

2. Claims 26 and 95

Claim 26 recites:

> 26. [a] The computer implemented method of claim 1, wherein said intercepting, by the at least one computer processor, further comprises:
>
> [b] triggering, by the at least one computer processor . . . initiating other actions comprising at least one of:
>
> [c] intercepting … a delete operation, and
>
> [d] determining … when to actually erase contents, wherein, at least one of:
>
> [e] an erasure comprises overwriting, by the at least one computer processor, at least one of content or at least a portion of a file with a predetermined pattern;
>
> [f] an erasure is triggered immediately, by the at least one computer processor . . . .

Ex. 1001, 36:39–62 (bracketed material and formatting added for clarity). Claim 95 recites similar elements. *See id.* at 50:38–56. Petitioner asserts Kung teaches these elements. *See* Pet. 71–73 (citing Ex. 1002 ¶¶ 279–284, 286). Specifically, Petitioner contends Nagar's disclosure of a filter driver that intercepts I/O requests and performs "various actions to modify, extend, or replace the functionality provided by the original recipient of the I/O request" teaches the "intercepting" including "triggering" other actions recited in claim elements 26[a] and [b]. *See* Pet. 71 (citing Ex. 1005, 51, 497–501). Petitioner also assets Kung teaches "determining" when to actually erase contents as recited in claim element 26[d] because the program determines which erasure method needs to be performed to erase the contents of the file. *Id.* at 72 (citing Ex. 1002 ¶ 281; Ex. 1005, 3:9-32). Finally, Petitioner contends Kung teaches an "erasure comprising overwriting" content or a portion of a file with a predetermined pattern by

disclosing a conventional secure erasure method that overwrites 0s and 1s over the entire data file many times to ensure that the stored information cannot be recovered and that a POSITA would have understood the method could be preset to overwrite the data with a predetermined pattern, such as with all 0's or all 1's, or alternating 0's and 1's. *Id.* (citing Ex. 1002 ¶ 282; Ex. 1008, 1:24–29). Petitioner contends Kung discloses the limitations of claim 95 for the same reasons set forth with respect to claim 26.

We have reviewed Petitioner's arguments and evidence and agree that Petitioner has shown that Kung discloses the limitations of claims 26 and 95. Pet. 71–73 (citing Ex. 1002 ¶¶ 279–284, 286).

Patent Owner makes a number of arguments in response, none of which we find persuasive. *See, e.g.,* PO Resp. 33–38; PO Sur-reply 19–20. First, Patent Owner contends Kung's encryption method does not "actually erase" content as required by the claims because Kung's encryption method retains content and merely deletes the file directory pointer and encrypts the file. *See, e.g.,* PO Resp. 34, 38 (citing Ex. 2001 ¶ 68; Ex. 1008, 3:67–4:7, Fig. 1). This argument is not persuasive because Petitioner also relies on Kung's disclosure of a conventional method of deleting a file by overwriting the file with 0's and 1's. We agree with Petitioner that overwriting a file a file with 0's and 1's "actually erase[s]" the file.

Patent Owner next argues that Kung teaches away from the conventional method of overwriting a file with 0's and 1's for the same reasons set forth in Section II.J.1 in connection with claims 16 and 81. PO Resp. 34–35 (citing Ex. 2001 ¶ 69). This argument is not persuasive for the same reasons stated in Section II.J.1.

Patent Owner also contends Kung does not teach overwriting a file with a "predetermined pattern" and that "overwriting the contents multiple times uniformly alternating between 0's and 1's" is inconsistent with the '243 patent which states a "secure erasure may be executed by overwriting the contents of a file with random patterns" and that the file may be overwritten only one time. *See* PO Resp. 35–36 (citing Ex. 2001 ¶¶ 69–70). We disagree with this argument and find that overwriting with 0's and then overwriting with 1's is a specific pattern. *See* Ex. 1002 ¶ 282 (stating that overwriting a file with 0s and then 1s is a pattern). The claims of the '243 patent do not require a single overwrite or the pattern to be random. *See also* Ex. 1001, 25:51–59 (stating that the "trap layer may allow the file to be deleted and may . . . repeat the overwrite operation several times, such as, . . . seven or fifteen times").

Patent Owner contends Kung does not disclose *determining* when to actually erase contents wherein an erasure is *triggered immediately* because Kung's secure deletion only occurs after *user* interaction and is not *triggered immediately. See* PO Resp. 37; Ex. 2001 ¶ 71

This argument is not persuasive. Claim element 26[f], which recites "an erasure is triggered immediately" is only one of the three "at least one" erasure options recited in claim 26. We agree with Petitioner that Kung teaches the erasure option recited in claim element 26[e], which recites "an erasure compris[ing] overwriting, . . . at least a portion of a file with a predetermined pattern." Thus, because Kung teaches the erasure option recited in claim element 26[e], Petitioner was not required to show that Kung discloses the erasure option recited in claim element 26[f].

We agree with Petitioner that Kung teaches *determining,* by the computer processor, when to actually erase contents recited in claim element 26[d], because Kung teaches that, after the user selects a secure deletion of the file (Ex. 1008, 3:9–32), the program, (and thus the processor) determines that that Kung's secure erasure method needs to be performed to erase the content of the file. Pet. 72 (citing Ex. 1002 ¶ 281).

Thus, for the foregoing reasons, Petitioner has shown that Nagar and Kung teach the limitations of claim 26, and the similar limitations of claim 95, which Patent Owner does not dispute separately. We also determine that Petitioner has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and Kung. Pet. 66–73; Ex. 1002 ¶¶ 266–278. We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 26 and 95 would have been obvious over the combination of Nagar and Kung.

K. Claims 6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 79, 82, 86, and 96 – Nagar and McGovern

Petitioner contends claims 6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 79, 82, 86, and 96 would have been obvious over the combined teachings of Nagar and McGovern. IPR608-Pet. 35–57; IPR608-Reply 9–15. Patent Owner responds that Nagar and McGovern do not disclose the limitations of claims 11 and 76 but does not dispute that the remaining claims (i.e., 6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75, 77, 79, 82, 86, and 96) would have been obvious over Nagar and McGovern. IPR608-PO Resp. 19–22; IPR608-PO Sur-reply 11–14.

Having considered the full record developed by trial, we are persuaded by Petitioner's arguments and evidence that claims 6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 79, 82, 86, and 96 would have been obvious over the Nagar and McGovern.

1. Claims 11 and 76

Claim 11, which depends directly from claim 10 and indirectly from claims 1 and 6, recites:

> [a] wherein said holding, by the at least one computer processor, the retained state comprises at least one of:
>
> [b] suspending, by the at least one computer processor, expiration of a retained state portion of the computer storage medium;
>
> [c] suspending, by the at least one computer processor, an unexpired retained state portion of the computer storage medium from entering an expired retained state;
>
> [d] suspending, by the at least one computer processor, clearing, by the at least one computer processor, of a read only attribute of the retained state portion of the computer storage medium by setting, by the at least one computer processor, a temporary attribute of the retained state portion of the computer storage medium; or
>
> [e] suspending, by the at least one computer processor, deletion, by the at least one computer processor, of an expired retained state portion of the computer storage medium.

Ex. 1001, 33:7–25 (bracketed material and formatting added for clarity). Claim 76, depends directly or indirectly from claims 66, 71, and 75. Claim 76 and its base claims recite limitations similar to those of claim 11 and its base claims. *Compare* Ex. 3002, 1; Ex.1001, 32:36–45, Ex.1001, 33:3–6 *with. id.* at 46:60–47:12, 47:37–45, 47:63–48:11.

Petitioner contends McGovern teaches the limitations of claims 11 and 76 by teaching extending a retention date/time in a committed WORM

file so as to suspend the expiration or deletion of a file. *See* IPR608-Reply 10; IPR608-Pet. 41–42, 45–47, 55 (citing, *inter alia*, Ex. 1006 ¶¶ 36, 127–128, Fig. 12; Ex. 1002 ¶¶ 222–225). Petitioner argues McGovern teaches a "write-once-read-many (WORM) system" that stores files with a specified retention date and allows setting a "retention policy" that can cause the system to observe "WORM properties (e.g., no deletion, no modifications) for the WORM file during the applicable retention period." IPR608-Pet. 35–36 (citing Ex. 1006 ¶¶ 20, 119; Ex. 1002 ¶ 204). Petitioner further asserts that retention periods can be set to any date so long as the date is further in the future than the existing date and that the extended period may be "'infinite,' 'indefinite or permanent.'" *Id.* at 46 (quoting Ex. 1006 ¶ 128; citing Ex. 1002 ¶ 223). Petitioner contends that extending the retention date suspends the expiration of the file because it "suspends the file from being deleted." *Id.* (citing Ex. 1002 ¶ 223).

Petitioner also contends it would have been obvious to implement McGovern's WORM file system in Nagar, both of which are built on top of Windows NT, to, *inter alia*, provide additional functionality for controlling access to files so files could be retained for specified time periods, such as retaining tax records for a certain number of years after each tax filing. *Id.* at 38–40 (citing Ex. 1005 ¶¶ 7, 9–10, 15, 20–21, 79, 89, 120–121; Ex. 2001 ¶¶ 207–210).

Patent Owner responds that the cited art does not disclose "holding . . . the retained state comprises at least one of" the "suspending" steps recited in claims 11 and 76. *See* IPR608-PO Resp. 19–22; IPR608-PO Sur-reply 11–14. Patent Owner contends claims 11 and 76 "do not claim setting a new, later retention date . . . but instead suspend expiration in holding the

retained state." IPR608-PO Resp. 20–21 (citing Ex. 1001, 21:60–67, 33:7–25, 47:66–11; Ex. 2001 ¶ 51). Patent Owner argues that "[a] POSITA would understand 'suspending' to mean temporarily setting aside or making inoperative the 'enforcing … a retention access privilege' of claims 6 and 71 of the '243 Patent, from which claims 11 and 76 indirectly depend, until such time as the suspension is lifted." *Id.* at 22 (citing Ex. 2001 ¶ 52). Patent Owner contends that the "suspending" of the '243 patent is substantively different than merely "changing" a retention date as show in McGovern because in McGovern's approach, there is no way to recover the previous system's behavior by lifting a suspension as in the '243 patent. *See id.* Patent Owner also argues that the approach claimed in the '243 patent is superior to what is shown in McGovern because the '243 patent's approach allows the system to "revert[] back to normal immediately" once the suspension is lifted, thereby "allowing the previous, still existing expiration dates to be applied." *Id.* at 21 (citing Ex. 2001 ¶ 51).

We disagree with Patent Owner's arguments because Patent Owner is relying on limitations that are not found in the claims. We disagree with Patent Owner that the term "suspending" excludes changing or extending the expiration date to a later date. The claims do not recite, or require either explicitly or implicitly, that the term "suspending" excludes changing or extending the expiration date to a later date. Claim 11 requires that "holding the retained state comprises at least one of" four different "suspending" steps (i.e., claim element 11[b]–[d]. For example, claim element 11[b] recites "suspending . . . expiration of a retained state portion of the computer storage medium." We determine that there is nothing in this limitation that

would exclude changing or extending the expiration date to a later date from being included in "suspending expiration."

To support its argument that claims 11 and 76 "do not claim setting a new, later retention date" but "instead suspend expiration in holding the retained state," Patent Owner cites to the specification of the '243 patent which states:

> According to an exemplary embodiment, the retention policy expiry may be suspended indefinitely in the event of litigation to prevent valuable files directories and documents from being accidentally destroyed while the litigation is still on going. According to an exemplary embodiment, the suspension may be a legal hold. In an exemplary embodiment, the legal hold may prohibit and/or inhibit the deletion of files even if their retention period is expired.

Ex. 1001, 21:60–67 (cited in IPR608-PO Resp. 21). We disagree that this exemplary embodiment limits the claims as argued by Patent Owner. Indeed, this embodiment relied upon by Patent Owner gives no indication that the term "suspension" in the '243 patent excludes changing or extending the expiration date to a later date. Rather, this paragraph describes suspending retention policy expiry indefinitely, so that the deletion of files is prohibited or inhibited. Moreover, Patent Owner does not address why McGovern's teaching of "[e]xtending the retention date infinitely" is different from the '243 patent's teaching of "the retention policy expiry [being] . . . suspended indefinitely."[19]

[19] Patent Owner does state that indefinitely "does not mean forever, but rather lasting for a period whose end is not established" but does not address how McGovern's indefinite suspension of expiration of a file is different from that taught in the '243 patent or required by claim 11. *See* Sur-reply 13.

The phrase "even if their retention period is expired," emphasized by Patent Owner (*see* IPR608-PO Resp. 22), does not support Patent Owner's assertion that "[d]uring the 'suspending' in holding the retained state in the '243 Patent, it does not matter if the retention date is in the past or future because the deletions will not be allowed." IPR608-PO Resp. 21–22. The paragraph does not say that "once the suspension is lifted in the '243 Patent, the system is capable of reverting back to normal immediately, allowing the previous, still existing expiration dates to be applied" or "[w]hen the suspension is lifted, the retention dates may be compared to the clock date and deletion allowance proceeds as originally scheduled," much less "[l]ifting of the suspension would result in re-enforcing the retention policy." *Id*. The "indefinitely" used in the paragraph actually means making the suspension unlimited by time, rather than Patent Owner's asserted "[l]ifting of the suspension" or "temporarily setting aside or making inoperative the 'enforcing … a retention access privilege' … until such time as the suspension is lifted." *Id*. at 22.

In its Sur-reply, Patent Owner also argue that if "suspending" means merely changing or extending an expiration date to a later date, then claim 11 "would make no sense." *See* IPR608-PO Sur-reply 12. Patent Owner contends the phrase "suspending deletion of an expired retained state" recited in claim element 11[e] requires an "expired retained state," which would "be impossible if suspending were defined to mean extending." *See id.* at 12–13. However, the step of "suspending expiration" does not include reference to the "expired retained state" and thus is not limited by the absent language.

Patent Owner also contends Petitioner failed to disclose which of the "suspending" alternatives recited in claim 11 is disclosed by McGovern. IPR608-PO Sur-reply 11–12. This argument is not persuasive because Petitioner provided this information on pages 45–47 of its Petition. *See* IPR608-Pet. 45 (identifying claim elements 11[b], [c], and [e] in the heading), *id.* at 46–47 (stating "McGovern's teaching of extending an expiration period for a WORM file constitutes at least one of" the suspending steps recited in claim elements 11[b], [c], or [e]).

We agree with Petitioner's argument and supporting evidence that McGovern teaches "suspending . . . expiration of a retained state" because McGovern teaches resetting the retention period to any date so long as it is "further in the future than the existing date." Pet. 46 (citing Ex. 1006 ¶ 128, Fig. 12).

Having considered the full record developed by trial, we are persuaded by Petitioner's contentions and evidence that Nagar and McGovern teach all of limitations of claims 11 and 76 and determine that Petitioner has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and McGovern. IPR608-Pet. 35–41, 45–47, 55.

We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 11 and 76 would have been obvious over the combination of Nagar and McGovern.

2. Claims 7, 8, 12, 14, 17, 21, 27, 65, 72, 73, 77, 79, 82, 86, and 96

Petitioner asserts claims 7, 8, 12, 14, 17, 21, 27, 65, 72, 73, 77, 79, 82, 86, and 96 would have been obvious over the combined teachings of Nagar and McGovern. IPR608-Pet. 35–57. Patent Owner does not separately

argue the patentability of these claims. *See generally* IPR608-PO Resp.; *see also* IPR608-Paper 12 (Scheduling Order), 7 (stating "any arguments not raised in the response may be deemed waived").

Having considered the full record developed by trial, we are persuaded by Petitioner's contentions and evidence that Nagar and McGovern teach all of limitations of claims 7, 8, 12, 14, 17, 21, 27, 65, 72, 73, 77, 79, 82, 86, and 96 and determine that Petitioner has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and McGovern. IPR608-Pet. 35–57; IPR608-Ex. 1002 ¶¶ 266–278.

We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 7, 8, 12, 14, 17, 21, 27, 65, 72, 73, 77, 79, 82, 86, and 96 would have been obvious over the combination of Nagar and McGovern.

L. Claims 18, 19, 83, and 84—Nagar and Vossen

Petitioner asserts claims 18, 19, 83, and 84 would have been obvious over the combined teachings of Nagar and Vossen. IPR608-Pet. 57–67. Patent Owner does not separately argue the patentability of these claims. *See generally* IPR608-PO Resp.; *see also* PR608-Paper 12 (Scheduling Order), 7 (stating "any arguments not raised in the response may be deemed waived").

Having considered the full record developed by trial, we are persuaded by Petitioner's contentions and evidence that Nagar and Vossen teach all of limitations of claims 18, 19, 83, 84 and determine that Petitioner has articulated reasoning with some rational underpinning that one of

ordinary skill in the art would have had reason to combine the teachings of Nagar and Vossen. IPR608-Pet. 57–66 (citing Ex. 1002 ¶¶ 260–266).

We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 18, 19, 83, and 84 would have been obvious over the combination of Nagar and Vossen.

M. Claims 5, 50, 64, 70, and 85—Nagar and Denning

Petitioner asserts claims 5, 50, 64, 70, and 85 would have been obvious over the combined teachings of Nagar and Denning. IPR608-Pet. 67–74 (citing Ex. 1002 ¶¶ 287–291). Patent Owner does not separately argue the patentability of these claims. *See generally* IPR608-PO Resp.; *see also* PR608-Paper 12 (Scheduling Order), 7 (stating "any arguments not raised in the response may be deemed waived").

Having considered the full record developed by trial, we are persuaded by Petitioner's contentions and evidence that Nagar and Denning teach all of limitations of claims 5, 50, 64, 70, and 85 and determine that Petitioner has articulated reasoning with some rational underpinning that one of ordinary skill in the art would have had reason to combine the teachings Nagar and Denning. IPR608-Pet. 67–74 (citing Ex. 1002 ¶¶ 287–291).

We, thus, determine that Petitioner establishes by a preponderance of the evidence that the subject matter of claims 5, 20, 64, 70, and 85 would have been obvious over the combination of Nagar and Denning.

N. Constitutionality of Inter Partes Review Proceedings

Patent Owner asserts that both *inter partes* review proceedings IPR2019-00607 and IPR2019-00608 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. *See, e.g.,* PO Resp. 22–23.

We decline to consider Patent Owner's arguments as the Federal Circuit has determined that *inter partes* review proceedings are not unconstitutional under the Takings Clause or Due Process Clause as argued by Patent Owner. *See Celgene Corp. v. Peter*, 931 F.3d 1342, 1362 (Fed. Cir. 2019), *cert. denied* 2020 WL 3405867 (June 22, 2020); *see also Arthrex, Inc. v. Smith & Nephew, Inc.*, 935 F.3d 1319, 1331–32 (Fed. Cir. 2019); *Sound View Innovations, LLC v. Hulu, LLC*, Nos. 2019-1865, 2019-1867, 2020 WL 3583556, *3 (Fed. Cir. July 2, 2020) (non-precedential).

III. CONCLUSION[20]

For the reasons discussed above, we determine Petitioner has proven, by a preponderance of the evidence, that some of the challenged claims of the '243 patent are unpatentable, as summarized in the following tables.

[20] 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. 16654 (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).

IPR2019-00607:

Claims	35 U.S.C. §	Reference/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–4, 24, 25, 32–37, 39, 54–57, 61–63, 66–69, 87–89, 93, 94, 101–103	102(a)	Nagar	1–3, 24, 25, 32, 33, 35–37, 39, 54–57, 61–63, 66–68, 87–89, 93, 94, 101, 102	4, 34, 69, 103
1–4, 24, 25, 32–37, 39, 54–57, 61–63, 66–69, 87–89, 93, 94, 101–103	103	Nagar	1–3, 24, 25, 32, 33, 35–37, 39, 54–57, 61–63, 66–68, 87–89, 93, 94, 101, 102	4, 34, 69, 103
16, 26, 81, 95	103	Nagar, Kung	16, 26, 81, 95	
Overall Outcome			1–3, 24, 25, 32, 33, 35–37, 39, 54–57, 61–63, 66–68, 87–89, 93, 94, 101, 102	4, 34, 69, 103

IPR2019-00608:

Claims	35 U.S.C. §	Reference/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 62, 66	102(a)	Nagar	1, 62, 66	
6-8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 79, 82, 86, 96	103	Nagar, McGovern	6–8, 10–12, 14, 17, 21, 27, 65, 71–73, 75–77, 79, 82, 86, 96	
18, 19, 83, 84	103	Nagar, Vossen	18, 19, 83, 84	
5, 20, 64, 70, 85	103	Nagar, Denning	5, 20, 64, 70, 85	

Claims	35 U.S.C. §	Reference/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
Overall Outcome			1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, 96	

IV. ORDER

Accordingly, it is:

ORDERED that in IPR2019-00607, claims 1–3, 16, 24–26, 32, 33, 35–37, 39, 54–57, 61–63, 66–68, 81, 87–89, 93–95, 101, 102 of the ’243 patent have been shown to be unpatentable;

FURTHER ORDERED that in IPR2019-00607 claims 4, 34, 69, and 103 of the ’243 patent have not been shown to be unpatentable;

FURTHER ORDERED that in IPR2019-00608, claims 1, 5–8, 10–12, 14, 17–21, 27, 62, 64–66, 70–73, 75–77, 79, 82–86, and 96 of the ’243 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.

For PETITIONER:

Erika Arner
Joshua Goldberg
Jason Stach
Cory Bell
FINNEGAN, HENDERSON,
FARRABOW, GARRETT & DUNNER LLP
Erika.arner@finnegan.com
joshua.goldberg@finnegan.com
Jason.stach@finnegan.com
Cory.bell@finnegan.com

Andrew Devkar
MORGAN LEWIS & BOCKIUS
Andrew.devkar@morganlewis.com

Diek Van Nort
MORRISON & FOERSTER
dvannort@mofo.com

For PATENT OWNER:

Gregory Donahue
Andrew DiNovo
DINOVO PRICE LLP
gdonahue@dpelaw.com
adinovo@dpelaw.com