

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

COHESITY INC.,
Petitioner,

v.

COMMVAULT SYSTEMS, INC,
Patent Owner.

IPR2021-00935
Patent 8,762,335 B2

Before KARL D. EASTHOM, JENNIFER MEYER CHAGNON, and
DAVID COTTA, *Administrative Patent Judges*.

COTTA, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Cohesity Inc. (“Petitioner”)¹ filed a Petition to institute *inter partes* review of claims 1–3, 6, 7, 9–11, and 13 of U.S. Patent No. 8,762,335 B2 (Ex. 1001, “the ’335 patent”). Paper 1 (“Pet.” or “Petition”). Commvault Systems, Inc. (“Patent Owner”)² filed a Preliminary Response. Paper 8 (“Prelim. Resp.”).

Under 35 U.S.C. § 314(a), *inter partes* review may not be instituted unless the Petition “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” We have reviewed the arguments and evidence of record. Based on the preliminary record, we find that Petitioner has established a reasonable likelihood that at least 1 of the challenged claims is unpatentable based on the grounds advanced in the Petition. Thus, for reasons explained below, we institute *inter partes* review of claims 1–3, 6, 7, 9–11, and 13 of the ’335 patent.

A. Related Patents and Proceedings

The parties identify the following lawsuit as relating to the ’335 patent: *Commvault Systems, Inc. v. Cohesity Inc.*, Case No. 1-20-cv-00525-MN (D. Del.). Pet. 72; Paper 4, 1. In addition, we note that the ’335 patent claims priority from an application that issued as U.S. Patent No. 8,447,728 (“the ’728 patent”). Ex. 1001, code (63). The ’335 and ’728 patents claim priority to a number of common applications. *Id.* The ’728 patent was

¹ Petitioner identifies itself as the real party-in-interest. Pet. 72.

² Patent Owner identifies itself as the real party-in-interest. Paper 4, 1.

challenged in IPR2021-00535, now terminated, and was involved in the following lawsuit, now dismissed: *Commvault Systems, Inc. v. Rubrik, Inc.*, Case No. 1-20-cv-00524-MN (D. Del.). IPR2021-00535, Paper 1, 1, Paper 4, 1.

B. Asserted Grounds of Unpatentability

Petitioner asserts two grounds of unpatentability in this Petition (Pet. 8), which are provided in the table below:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–3, 6, 7, 9–11, 13	103(a) ³	Kahn ⁴
3, 7, 11	103(a)	Kahn, Forney ⁵

Petitioner relies on the declaration of Dr. Erez Zadok, among other evidence. Ex. 1003. Patent Owner responds with a declaration from Mark T. Jones, Ph.D., along with other evidence. Ex. 2002.

C. Technology Overview & the '335 Patent

The '335 patent is titled “System and Method for Storage Operation Access Security,” and concerns controlling access to stored data, using a pre-existing security infrastructure to provide proper access control for data

³ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. §§ 102 and 103. Based on the filing date of the '335 patent, we apply the pre-AIA versions of §§ 102 and 103.

⁴ Kahn, U.S. 7,185,192 B1, issued Feb. 27, 2007 (Ex. 1004).

⁵ Forney et al., U.S. 8,559,605 B2, issued Oct. 15, 2013 (Ex. 1005, “Forney”).

stored outside its original location, such as a backup copy of that data.

Ex. 1001, code (57), 2:52–55.

The '335 patent describes problems with prior art backup systems, including that “[s]econdary copies of data are often stored in a publicly accessible location for quick restoration of data in the event of a disaster or other data loss event,” but “[b]acked up data may contain sensitive information that is more widely accessible than the original data.” Ex. 1001 at 1:62–2:2. Thus, “[b]acking up data often removes the data from the well-planned security environment in which it was originally stored.” *Id.* at 2:2–4. The '335 patent teaches that there is a need to address this problem. *Id.* at 2:17–18.

To address this need, the '335 patent discloses a “method and system for controlling access to stored data.” *Id.* at code (57). In the method of the '335 patent, when the “storage access control system receives a request to perform a storage operation that makes data at a source location available at a destination location . . . , the storage access control system queries the source or other location for access control information.” *Id.* at 2:55–3:2. For example, “[t]he file system may contain access information that identifies the users and groups that have access to the data” and that can be stored along with the file. *Id.* at 3:5–9. “Then, the storage access control system applies the access control information to the data stored at the destination location.” *Id.* at 3:9–11. “In the example of backing up files, the storage access control system may place similar access control restrictions on the backup files that existed on the original files.” *Id.* at 3:16–19. “In this way, the backed up data is given similar protection as that of the original

data.” *Id.* at 3:19–20.

The storage access control system may store access control information as an Access Control List (“ACL”), where the ACL contains a list of users and/or groups that are allowed or denied access to data. *Id.* at 4:27–32. “In some embodiments, the storage access control system assigns access rights based on the content of or metadata associated with a data object, such as by querying a content or metadata indexing system.” *Id.* at 5:3–6. In other embodiments, “the preexisting security system may maintain a list of computers associated with a particular user, and the storage access control system can grant the user access, for example, to backup computers in that list.” *Id.* at 5:38–42.

D. Challenged Claims

The ’335 patent includes eighteen claims. Of those, claims 1–3, 6, 7, 9–11, and 13 are challenged here. Pet. 1. Independent claim 1 is illustrative of the claims challenged in this Petition and is reproduced below with bracketing added corresponding to the labeling used by Petitioner to refer to various claim elements:

1. [Pre] A method for execution by at least one processor to manage users in a data management system, wherein the data management system manages secondary copies of data files, the method comprising:
 - [a] adding a user of the data management system to a previously created group within the data management system, wherein the group associates one or more users with at least one access right for performing storage operations;

[b] receiving a request from the user to perform a storage operation, wherein the storage operation is to create a secondary copy of a production data file;

[c] causing a security system to be queried to determine access rights of the user,

wherein the access rights relate to the user's rights to access the production data file, and,

[d] causing the requested storage operation to be performed when the access rights permit the user to request the requested storage operation,

[e] wherein the secondary copy is used to restore production data from the production file from which the secondary copy is created;

[f] wherein causing the security system to be queried to determine the access rights includes determining one or more computers through which the user has access,

[g] wherein the access rights permit the data management system to perform the requested storage operation if the production data file is associated with one of the determined one or more computers;

[h] wherein adding the user to the created group within the data management system includes associating the created group with the user in the security system; and

[i] wherein the at least one access right for performing storage operations determines which data a user within the group can access.

Ex. 1001, 10:58–11:28.

II. ANALYSIS

A. Principles of Law

“In an [*inter partes* review], 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 *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)).

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the subject matter sought to be patented 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 that 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) secondary considerations of nonobviousness when presented. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Person of Ordinary Skill in the Art (“POSA”)

In determining the level of skill in the art, we consider the problems encountered in the art, the art’s solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986).

Citing the declaration of Dr. Zadok, Petitioner contends that a POSA would have “at least a Bachelor’s Degree in an Engineering discipline such as Electrical, Computer, or Software Engineering, or a Bachelor’s Degree in Computer Science, Information Systems, or equivalent degree, and at least

two years of relevant experience in the research, design, development or administration of data storage systems.” Pet. 7 (citing Ex. 1003 ¶¶ 88–89). Petitioner further explains that “additional education” could “substitut[e] for less experience and *vice versa*.” *Id.*

In the Preliminary Response, Patent Owner does not oppose Petitioner’s proposal, nor does it offer a proposal of its own. *See generally* Prelim. Resp. Notably, Patent Owner’s declarant, Dr. Jones, accepts Petitioner’s definition of the POSA. Ex. 2002 ¶ 20 (“For purposes of this declaration, I accept Dr. Zadok’s proposed qualifications of a [POSA].”).

Petitioner’s definition of the POSA is consistent with the specification of the ’335 patent and the prior art currently of record. Accordingly, we adopt it for purposes of this Decision. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (explaining that specific findings regarding ordinary skill level are not required “where the prior art itself reflects an appropriate level and a need for testimony is not shown”) (quoting *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 163 (Fed. Cir. 1985)).

C. Claim Construction

We interpret a claim “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).” 37 C.F.R. § 42.100(b) (2020). Under this standard, we construe the claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” *Id.*

The parties do not propose a particular construction for any claim term. Pet. 9; *see* Prelim. Resp.

In the course of our discussion, we highlight several claim construction issues that the parties may wish to address. However, at this stage in the proceeding, we determine that no explicit construction of any claim term is necessary to resolve the issues necessary to determine whether to institute review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 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))); *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011) (“[C]laim terms need only be construed ‘to the extent necessary to resolve the controversy’”).

D. Overview of the Asserted Prior Art

1. Kahn (Exhibit 1004)

Kahn is a U.S. Patent issued on February 27, 2007. Ex. 1004, code (45). Kahn discloses “systems and techniques which provide enhanced access control to resources in a computing system environment.” *Id.* at 1:6–9. Figure 2 of Kahn is reproduced below.

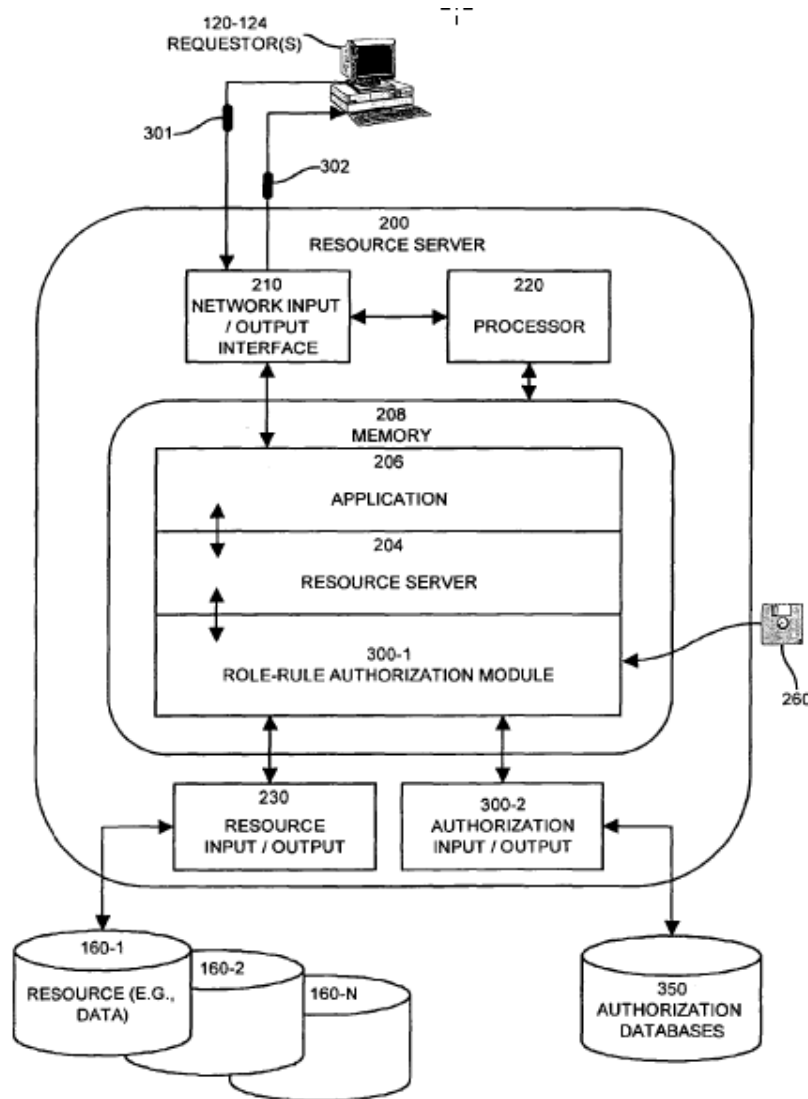


FIG. 2

Figure 2 of Kahn depicts “an example high-level architecture of a resource server equipped with a role/rule based access control system.” *Id.* at 9:59–61. As shown above, Kahn’s system uses processor 220 within resource server 200 for processing requests 301 made by requestors 120–124 (computer users from various departments). *Id.* at 16:5–13; *see id.* at 10:27–29. In operation, resource server 200 receives request 301 from requestor 120–124 for access to one or more resources 160-1 . . . N (e.g., data), and

network input/output interface 210 passes the request 301 to software application 206, which forwards the request to resource server 204. *Id.* at 16:63–17:5; *see id.* at 10:29–32, 26:67–27:2, Fig. 6, step 400. Resource server 204 forwards the request 301 to role-rule authorization module 300-1 via an application programming interface (API). *Id.* at 17:5–10. Role-rule authorization module 300-1 receives and examines the request 301 and, based thereon, selects one or more filter operations and a set of rules from authorization databases 350 for producing access control decision 302. *Id.* at 17:28–35. For example, the request 301 might specify that a particular requestor 120–124 acting in a Backup Operator role needs access to copy or backup a volume of storage in the data storage system resource 160-1. *Id.* at 15:17–27 (Table 1), 17:35–41. Once role-rule authorization module 300-1 has selected or determined what rules apply, it performs rule operations in the selected set of rules to determine the access control decision 302, which is provided—with or without the requested data—back to the requestor 120–124. *Id.* at 16:15–17, 17:41–46.

Figure 3 of Kahn is reproduced below.

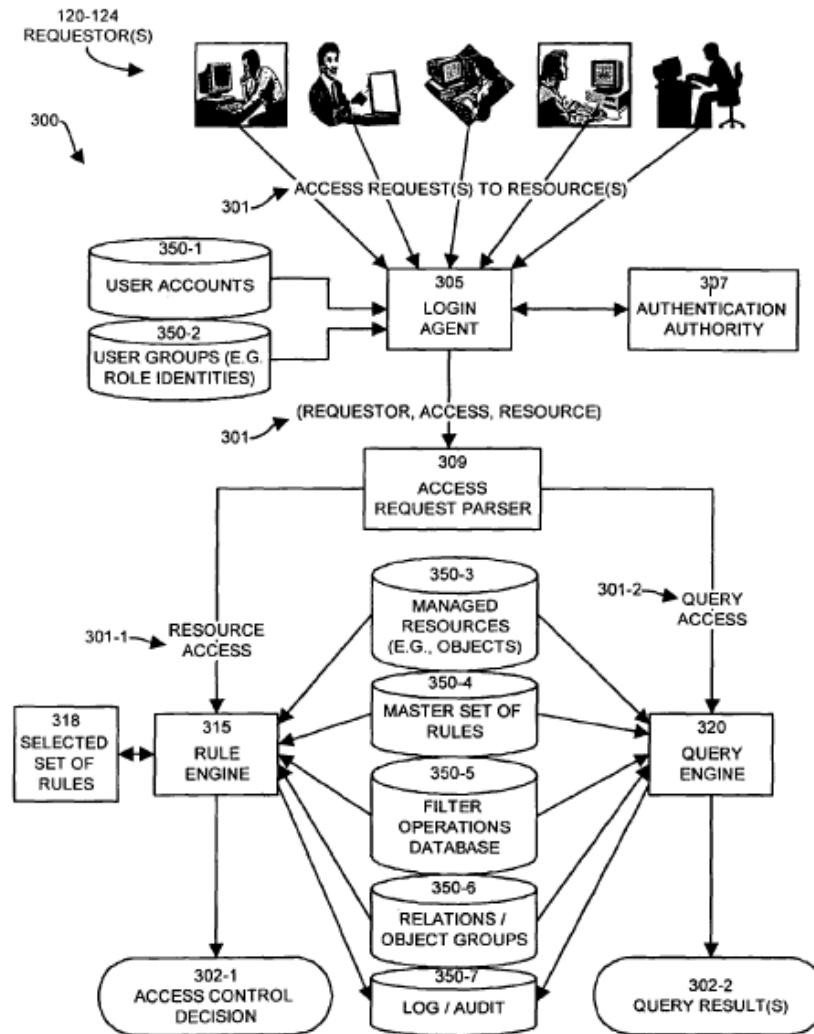


FIG. 3

Figure 3 of Kahn depicts “an example software architecture . . . of the role/rule-based access control system.” *Id.* at 9:63–65. The authorization system 300 includes various authorization databases 350 that are used to produce an access control decision 302, the databases including, for example, a user accounts database 350-1, a master set of rules 350-4, and a filter operations database 350-5. *Id.* at 18:6–9, 18:18–20. As shown in

Figure 3, access request parser 309 parses an access request 301 and passes the requestor, access and resource information to either a rule engine 315 or query engine 320. *Id.* at 18:55–63. From the master set of rules 350-4, rule engine 315 may use filter operations from database 350-5 to select a subset of rules 318 defining certain rule operations. *Id.* at 10:35–44, 17:29–35 27:2–8, Fig. 6, step 401. “[F]ilter operations are used to filter out or pre-select which rules from the master set of rules 350-4 apply to certain criteria within the current access request.”⁶ *See id.* at 21:56–58. The system then applies the access request 301 against the selected subset of rules 318 to determine an access control decision 302. *Id.* at 10:44–47, 27:8–29, Fig. 6, steps 402, 403. Rule operations, for example, may grant or deny specific permissions to the requestor for the specific resource. *Id.* at 10:47–49.

⁶ Here and throughout, for readability, we omit to bold quoted reference numbers that are bolded in the original.

Figure 5 of Kahn is reproduced below.

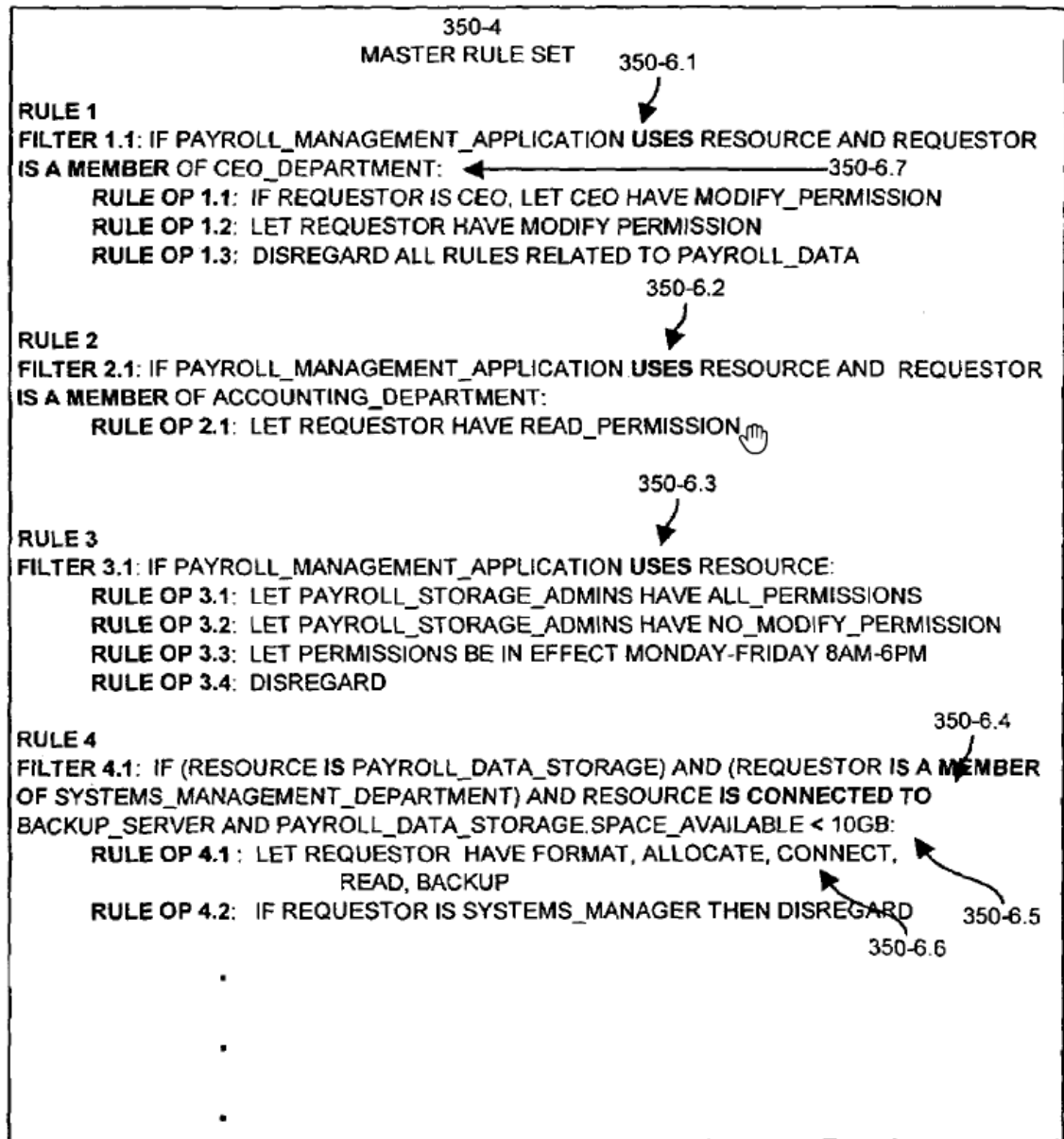


Figure 5 of Kahn depicts an example of a subset of rules 318 excerpted from the master set of rules 350-4. For example, Rule 4 comprises filter operation 4.1, which determines: 1) if the resource (from the access request 301) is payroll data storage, for example a storage device 160 that stores payroll data, 2) if the requestor is a member of the systems management department

(defined in group database 350-6), 3) if the resource is connected to a backup server, and 4) if the space available is less than 10 gigabytes. *Id.* at 25:2–14. If the above conditions are met, rule engine 315 may provide the requestor (for example, a systems manager) with, among other things, “BACKUP” permission, which allows the systems manager to read and backup the payroll data. *Id.* at 25:14–21.

2. Forney (Exhibit 1005)

Forney is a U.S. Patent issued on Oct. 15, 2013. Ex. 1005, code (45). Forney discloses an integrated communication system (ICS) that “integrates different types of messaging so that a user of the ICS can access all of the message types (e.g., voice mail messages, electronic mail or email messages, etc.) with a single message interface (also referred to as a ‘user interface’ or ‘UI’).” *Id.* at 12:45–49; *see id.*, Abstract, 1:58–60. The ICS may include a Messaging Communication Server (MCS), an interface module (IM), and an MCS Management Console. *Id.* at 14:41–51, Fig. 6-X, items 600-X, 610-X, 620-X, 660-X. The IM may run under control of a messaging server (MSERV) and couples to components of the MCS, the MCS Management Console, the MSERV, and a Database. *Id.* at 14:51–58, Fig. 6-X, items 610-X, 620-X, 640-X, 644-X, 660-X. The MCS and MSERV couple to the LAN for communication with other components. *Id.* at 14:58–60, Fig. 6-X.

In addition, the run time component (RTC) of the IM may translate communications between components of the MCS and components of the MSERV, for example, by “retriev[ing] user information from the directory service (e.g., Active Directory) of a groupware application in response to a request from the MCS.” *Id.* at 17:15–19. According to Forney, “[t]he

MSERV also couples to a directory service . . . , which is a database of information on each user account in the enterprise network system.” *Id.* at 17:53–54. Forney also describes that “[i]n embodiments including (AD) [an active directory], there is a user object stored in an AD Database for each enterprise user” with “many fixed attributes such as user name, user phone number, user mailbox location, and user email address.” *Id.* at 19:6–11. Such user information may be used to direct a message from the messaging server and the cache to one or more client devices on any of the networks. *Id.*, Abstract. Fig. 2-X, step 212-X, 12:41–44.

Forney describes as well that, “[f]or security reasons, . . . communications with the MCS may be restricted to network components having particular known addresses” and “may require authentication by passcode or other security measures for certain kinds of access, for example, for access by the administrator,” where “[s]ecurity may also or alternatively be encrypted and/or provided by requiring a physical connection between the MCS and other component.” *Id.* at 25:61–26:5.

E. Obviousness over Kahn (Ex. 1004)

Petitioner asserts that claims 1–3, 6, 7, 9–11, and 13 are unpatentable as obvious over Kahn. Pet. 16–61; *see id.* at 16–46 (claim 1), 46–57 (claims 2, 3, 6, and 7, which depend ultimately from claim 1), 57–61 (claims 9–11 and 13, which Petitioner argues are obvious for substantially the same reasons as with claims 1–3 and 6). Patent Owner contends that Kahn does not disclose certain elements of claim 1.

Petitioner shows, based on this preliminary record, where each of the

limitations of the challenged claims is taught or suggested by Kahn.

Pet. 16–61. Petitioner’s assertions above are backed by the cited prior art and by the testimony of its declarant, Dr. Zadok. *Id.*; *see also* Ex. 1003

¶¶ 101–209. On this preliminary record, we determine that Petitioner’s arguments and evidence are sufficient for purposes of institution. We focus our discussion on the elements of the challenged claims that Patent Owner contends are not disclosed or suggested by Kahn.

Claim 1 requires, among other things, “causing a security system to be queried to determine access rights of [a] user, wherein the access rights relate to the user’s rights to access the production data file, and . . . wherein causing the security system to be queried . . . includes determining one or more computers through which the user has access.” Ex. 1001, 11:5–18.

Patent Owner argues that Petitioner “fails to show any disclosure of ‘quer[ying] to determine . . . the user’s rights to access [a] file’ that ‘includes determining one or more computers through which the user has access,’” as recited in limitations 1[c] and 1[f]. Prelim. Resp. 5 (alterations in original). On this preliminary record, we do not find this argument persuasive.

As an initial matter, none of the claims recite “querying to determine the user’s rights to access a file” as Patent Owner appears to contend. Rather, the claims are broader, requiring that the “security system be queried to determine access rights of the user,” and that the “access rights **relate** to the user’s rights to access the production data file.” Ex. 1001, 11:5–8 (emphasis added). On the current record, we do not find it necessary to construe the phrase “relate to the user’s rights to access the production data file” to determine whether to institute review. Nonetheless, we flag the issue

in the event the parties wish to address the proper construction of this phrase at trial.

Turning to the issue of whether Kahn discloses a query to determine access rights that relates to a user's rights to access a production data file, Kahn discloses that "[a]ccess requests can specify, for example, an identity of a requestor, a type of access requested, and a resource to which this requester requests the access." Ex. 1004, 10:29–33. Kahn's security system then "applies the access request against [a] selected set of rules" that "might, for instance, grant or deny specific permissions to the requestor for the specific resource." *Id.* at 10:44–49; *see also id.* at 17:35–41 (explaining that the access request "might specify, for example, that a particular requestor . . . needs a specific type of access, such as the ability to configure, copy or backup a volume of storage in the data storage system resource"). Kahn also discloses that the resources in the access requests that its system manages include, among other things, "objects for files." *Id.* at 20:32–39; *see also id.* at 20:39–47 (teaching that the "authorization system **300** can treat each portion of data (e.g., records, files, databases, software applications, etc.) . . . as an accessible resource with respect to access control and authorization"). Accordingly, the preliminary record supports Petitioner's assertion that Kahn "discloses that a security system (*e.g.*, the role-rule authorization module) can be queried to determine the particular access rights permitted to a particular user (*e.g.*, for access to a file for backup purposes)." Pet. 30.

With respect to the requirement that the access rights query includes determining "one or more computers through which the user has access,"

Kahn's exemplary "group definition" (cited at Pet. 38–39) discloses a "list of members (e.g., other object resources 350-5 such as computer users, software applications, **computers** or other entities) that are considered, for access control purposes to be in the CEO/Executive department." Ex. 1004, 22:27–35 (emphasis added). Kahn then teaches using membership in a group in making access determinations. For example, Kahn's discussion of Rule 4 states:

[R]ule 4 provides an example of . . . filter operation 4.1. This filter operation 4.1 determines that if the resource (from the access request 301) is payroll data storage (e.g., one of the storage devices 160 that stores payroll data) and the requestor is a member of the systems management department (i.e., defined as a group definition, stored in group database 350-6) and the resource is connected to a backup server (e.g., also be defined as a group of backup servers in database 350-6) and space available (an attribute of the object representing the payroll data storage device) is less than 10 gigabytes, then the rule engine 315 provides the requestor (presumably a systems manager if this filter operation is met) with "FORMAT" "ALLOCATE" "CONNECT" "READ" and "BACKUP" permissions. Such permissions allow the systems manager to format new disks, allocate space to the payroll data storage system and connect the new space to system, as well as to read and backup the payroll data.

Ex. 1004, 25:3–21. As set forth in the above passage, Rule 4 grants access if the following four requirements are met: 1) the resource is payroll data storage, 2) the requestor is a member of the systems management department, 3) the resource is connected to a backup server, and 4) space is available. Because Kahn includes computers in the group membership definition, and because Kahn considers group membership (i.e., membership

in the systems management department) in making access rights determinations, this disclosure supports Petitioner's position that Kahn discloses that access rights queries include determining "one or more computers through which the user has access." Patent Owner argues that users within a membership group may not have access to every computer in the group (Prelim. Resp. 20), but claim 1 does not require that. Rather, on this preliminary record, we find it sufficient that Kahn's access right query includes considering whether a computer is part of a membership group.

In addition, Petitioner asserts that "payroll data storage," as recited in Rule 4, is a "computing device." Pet. 39–40. Kahn considers whether a resource is "payroll data storage" as a condition for granting access rights. Ex. 1004, 25:3–21. On this preliminary record, this provides another way in which Kahn confers access by "determining one or more computers through which the user has access." Patent Owner contends that Petitioner fails to provide evidentiary support for its assertion that "payroll data storage" is a computing device. Prelim. Resp. 17–18 (citing Ex. 2002 ¶¶ 50–51). Although we recognize some ambiguity in Petitioner's assertion, Kahn's use of the term "payroll data storage" and of element 160 throughout its specification appears to support Petitioner's assertion. Dr. Jones' testimony in this regard is not persuasive on this preliminary record because it considers the term "payroll data storage" and element 160 in isolation. Ex. 2002 ¶¶ 50–51. To the extent Patent Owner continues to assert that "payroll data storage" and element 160 do not encompass computers, Patent Owner is invited to further develop the record on this point at trial.

Petitioner also contends that Kahn discloses “determining one or more computers through which a user has access” by disclosing examples where “access to a given host or computer is necessary for an access request, including for backup operations.” Pet. 40. On this preliminary record, Kahn supports Petitioner’s position. Kahn’s Table 1 discloses that a requestor in the role of a “Backup Operator” is provided access to a “host, such as UNIX, NT, MVS” in order to perform backup operations. Ex. 1004, 15:17–28. In this regard, we note that the ’335 patent defines the term “computer” to encompass a “host.” Ex. 1001, 7:8–11 (“[T]he terms ‘computer,’ ‘host,’ and ‘host computer’ are generally used interchangeably herein, and refer to any of the above devices and systems, as well as any data processor.”). Accordingly, with Kahn’s reference to UNIX as performing backup operations, we consider the “host” in Kahn’s Table 1 to be a computer through which the user has access to particular files. To the extent Patent Owner contends that the term “computer,” as recited in claim 1, does not encompass a “host,” as described in Kahn’s table 1, Patent Owner is invited to brief the issue at trial.

Finally, Petitioner supports that Kahn discloses “determining one or more computers through which a user has access” by pointing to Kahn’s general teaching that its access control mechanisms are applicable for providing control over many types of resources, including e.g. a computer system. Pet. 41 (citing Ex. 1004, 32:48–63). According to Petitioner this supports that the queried access rights in Kahn “include[] computers through which the user accesses the production file.” *Id.* (citing Ex. 1003 ¶¶ 150–160). The cited disclosure in Kahn is consistent with the disclosures

discussed above and, on this preliminary record, we agree with Petitioner that it lends support to its contention that Kahn determines access rights by determining “one or more computers through which the user has access.”

Patent Owner argues that Petitioner “fails to demonstrate that any of the supposed ‘determining one or more computers’ teachings it relies upon are a part of ‘quer[ying] to determine ... *the user’s rights to access the production data file*.’” Prelim. Resp. 8. More specifically, Patent Owner argues that Rule 4 “has nothing to do with querying to determine the ‘user’s rights to access the production data *file*.” *Id.* at 11. Patent Owner contends that the access request at issue in Rule 4 is a “request to a particular ‘*resource*,’ namely ‘*payroll data storage . . .*’” and thus the “access request” “is not requesting access to a ‘production data file,’ but, rather, to a storage device (e.g., a disk).” *Id.* at 11–12.

As an initial matter, we do not understand the access rights query recited in claim 1 to require determining one or more computers to determine the user’s rights to access the production data file. Rather we understand the claim language to require that the access rights query:

- 1) “relate to the user’s rights to access the production data file,” and
- 2) “include[] determining one or more computers through which the user has access.” Ex. 1001, 11:5-8, 15–18. On the current record, we do not find it necessary to construe the language recited in elements 1[c], 1[d], and 1[f]. Nonetheless, we flag the issue in the event the parties wish to address the proper construction of this phrase at trial.

Turning to Kahn’s disclosure, the preliminary record supports that Kahn discloses querying to determine access rights where that query

includes determining one or more computers through which the user has access and relates to a user's right to access a particular file. Patent Owner's arguments to the contrary interpret the scope of Kahn's disclosure too narrowly. Kahn discloses an "access control mechanism" that provides access control for a variety of resources, including files. Ex. 1004, 32:48–63 (cited at Pet. 41); *see also id.* at 20:32–52. As discussed above, one of the ways in which this "access control mechanism" operates is by "determining one or more computers through which the user has access." *See* Ex. 1003 ¶¶ 150–160. This is a sufficient connection, on this preliminary record, to support that Kahn access rights query includes "determining one or more computers" and "relate[s] to a user's rights to access [a] production data file."

Beyond the general disclosures cited in the Petition, on this preliminary record, the end result of the specific examples of "determining one or more computer" that Petitioner relies upon appear to "relate to the user's rights to access the production data file." For example, Rule 4 "determines one or more computers" as part of determining whether to grant permission to "read and backup the payroll data" (Ex. 1004, 25:3–21) and table 1 of Kahn "determines one or more computers" as part of determining whether to provide access to "back up X to tape" (*id.* at 15:18–28). On this preliminary record, we understand granting backup permission with respect to data to "relate to the user's rights to access" the files in which such data is maintained.

Claim 1 requires that the access rights "permit the data management system to perform the requested storage operation if the production data file

is associated with one of the determined one or more computers.” Ex. 1001, 11:19–22. Patent Owner argues that Petitioner “fails to cite, and Kahn does not disclose, any rule in Kahn that would result in an access determination permitting a storage operation for a production data file ‘if the production data file is associated with’ a ‘computer through which the user has access.’” Prelim. Resp. 26. Patent Owner argues that claim limitation 1[g] “is not met by a system that simply determines that the user has access to a file, also has access to a computer, and the user uses the computer to access the file.” *Id.* at 29–30. According to Patent Owner, limitation 1[g] instead requires “that a decision whether to grant a storage operation to create a secondary copy of a production file be based on whether there is an ‘association’ between that ‘file’ and at least one of the determined computers.” *Id.* at 30 (quoting Ex. 2002 ¶ 73). On this preliminary record, we do not find this argument persuasive.

As an initial matter, we do not read the claims as narrowly as suggested in Patent Owner’s Preliminary Response. In particular, we do not read the claims to require that the determination as to whether to grant permission to perform a storage operation be “based on” whether a file is associated with a computer. Rather, the plain language of the claim requires only that when the condition set forth in limitation 1[g] — i.e., “if the production data file is associated with one of the determined one or more computers” — is met, then the access rights must “permit the data management system to perform the requested storage operation.” Ex. 1001, 11:19–23. Thus the claims are satisfied so long as access rights permit the requested storage operation in instances where the condition of limitation

1[g] is met, as is the case in e.g., Kahn’s Rule 4. *See, e.g.*, Ex. 1001, 25:3–21. On the current record, we do not find it necessary to construe the language recited in element 1[g]. Nonetheless, we flag the issue in the event the parties wish to address the proper construction of this phrase at trial.

Regardless of whether limitation 1[g] requires it, we find that the preliminary record supports that Kahn discloses determining whether to grant permission to perform a storage operation based on whether there is an association between a production file and at least one of the determined computers. For example, Rule 4 specifies that “BACKUP permission[.]” (which we understand to be a storage operation) is granted if the access control system determines, among other things: 1) that the resource to which access is requested is “payroll data storage” (which may include a file), and 2) that the requestor is a member of the “systems management department” as defined by a group definition (as discussed *supra*, the group definition may include a computer). Ex. 1004, 22:27–38, 25:3–22. The computer that is found to be a member of the systems management department is “associated” with a file in payroll data storage because both the computer and the file are conditions precedent for granting BACKUP access permission.⁷ For this reason, the preliminary record supports that Kahn’s Rule 4 meets limitation 1[g].

⁷ To the extent either party contends that Kahn does not disclose a production file associated with one or more computers, we invite them to brief whether Kahn nonetheless meets limitation 1[g]. *See Ex. Parte Schulhauser*, Appeal No. 2013-007847 (precedential) (holding that contingent claim limitation need only occur if the contingency is met).

In addition, Dr. Zadok testifies that Rule 4 meets limitation 1[g] because when Kahn’s “systems manager is permitted to perform the storage (*e.g.*, backup) operation, the data intended for backup (*e.g.*, the payroll data, which a [POSA] would understand could also be a file) is stored and resides on the computer system (*e.g.*, the payroll data storage device) through which the user accesses the payroll data, and therefore the data is also ‘associated’ with that computer.” Ex. 1003 ¶ 162. We agree with Dr. Zadok’s reasoning and find that, on this preliminary record, Dr. Zadok’s testimony is supported by Kahn’s disclosure. For this additional reason, we find that the preliminary record supports that Kahn discloses limitation 1[g].

Patent Owner argues that Petitioner “fails . . . to demonstrate that anything in Kahn’s alleged ‘*data management system*’ *performs* a storage operation” neglecting to identify “any part of Kahn’s alleged ‘data management system’ [that] . . . actually *performs* this storage operation.” Prelim. Resp. 31. According to Patent Owner, “Petitioner’s failure is understandable as Kahn never teaches that its alleged ‘data management system’ performs any storage operation.” *Id.* at 32. Patent Owner’s declarant explains that “[w]hile Khan does make several mentions of backup and copy permissions being requested or required for different rolls, [he] see[s] no disclosure in Kahn of any backup or copying of data actually being performed by Kahn’s alleged ‘data management system.’” Ex. 2002 ¶ 78. On this preliminary record, we do not find this argument persuasive.

The ’335 patent identifies backing up data from one computer to another as an example of a “storage operation.” Ex. 1001, 2:55–60. As discussed above, Kahn discloses an authorization system that allows the user

to backup data if certain preconditions are met. *See, e.g.*, Ex. 1004, 25:3–22. Kahn thus discloses a system that authorizes a user to perform a “storage operation.” The preliminary record does not support Patent Owner’s argument that Petitioner did not identify the specific part of Kahn’s system that performs the backup operation because Petitioner asserts, with citation to supporting evidence, that Kahn’s data management system is “embodied in a computer system, and includes at least one ‘processor’ (i.e., 220 processor) within a Resource Server 200’ of the computer system.” Pet. 18 (citing Ex. 1004, Figs. 2 & 3, 34:14–48 (claim 6)). On this preliminary record, the computer system in Kahn that Petitioner identifies as corresponding to the claimed “data management system” is sufficiently broad to encompass the specific entity that performs any authorized backup operation.

In sum, Petitioner shows, based on this preliminary record, where each of the limitations of the challenged claims is taught or suggested by Kahn. Pet. 16–61. For the reasons set forth above, the preliminary record does not support Patent Owner’s arguments that Petitioner failed to demonstrate that Kahn taught or suggested certain elements of claim 1. Accordingly, we determine that Petitioner has established a reasonable likelihood that at least 1 of the challenged claims is unpatentable as obvious over Kahn.

F. Obviousness over Kahn (Ex. 1004) and Forney (Ex. 1005)

Petitioner asserts that, to the extent it is determined that Kahn does not expressly disclose the additional limitations of claims 3, 7, and 11, these

limitations would have been obvious over Kahn and Forney. Pet. 61–66 (citing Ex. 1005, Abstract, 1:64–2:4, 12:45–49, 17:17–18, 18:30–32, 18:62–65, 19:6–11, 25:61–26:8). Petitioner provides documentary and testimonial evidence to back its assertions. *Id.*; see Ex. 1003 ¶¶ 210–226. Patent Owner does not contest this ground separately with particularity beyond the arguments presented for independent claim 1 with regard to the first ground. *See generally* Prelim. Resp. Also, if trial is instituted it must be instituted on all challenged claims and grounds. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1354 (2018).

III. CONCLUSION

On this preliminary record, Petitioner has established a reasonable likelihood of prevailing in showing that at least one of the challenged claims is unpatentable based on the grounds advanced in the Petition.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *granted*, and we institute *inter partes* review of claims 1–3, 6, 7, 9–11, and 13 based on the grounds asserted in this Petition;

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is given of the institution of trial, which will commence on the entry date of this Decision.

IPR2021-00935
Patent 8,762,335 B2

For PETITIONER:

David B. Cochran
Matthew W. Johnson
Marlee R. Hartenstein
JONES DAY
dcochran@jonesday.com
mwjohnson@jonesday.com
mhartenstein@jonesday.com

For PATENT OWNER:

Kenneth J. Weatherwax
Bridget Smith
Flavio Rose
Parham Hendifar
Patrick Maloney
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
smith@lowensteinweatherwax.com
rose@lowensteinweatherwax.com
hendifar@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com