

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

IPR2020-00661
Patent 8,191,158 B2

Before MICHAEL R. ZECHER, NABEEL U. KHAN, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

OGDEN, *Administrative Patent Judge*.

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

I. INTRODUCTION

In response to a Petition (Paper 2, “Pet.”) by Petitioner Dolby Laboratories (“Dolby”), the Board instituted an *inter partes* review of claim 4 of U.S. Patent No. 8,191,158 B2 (Ex. 1001, “the ’158 patent”). Paper 13. Patent Owner Intertrust Technologies Corporation (“Intertrust”) filed a Patent Owner Response (Paper 17, “PO Resp.”), Dolby filed a Reply to the Patent Owner Response (Paper 20, “Pet. Reply”), and Intertrust filed a Sur-reply (Paper 21, “PO Sur-reply”).

We held an oral hearing on July 13, 2021, and the transcript is entered on the record. Paper 27 (“Tr.”).

This is a Final Written Decision under 35 U.S.C. § 318(a) as to whether the claim challenged in the *inter partes* review is patentable. By a preponderance of the evidence on the record before us, Dolby has shown that challenged claim 4 of the ’158 patent is unpatentable.

II. BACKGROUND

A. RELATED PROCEEDINGS

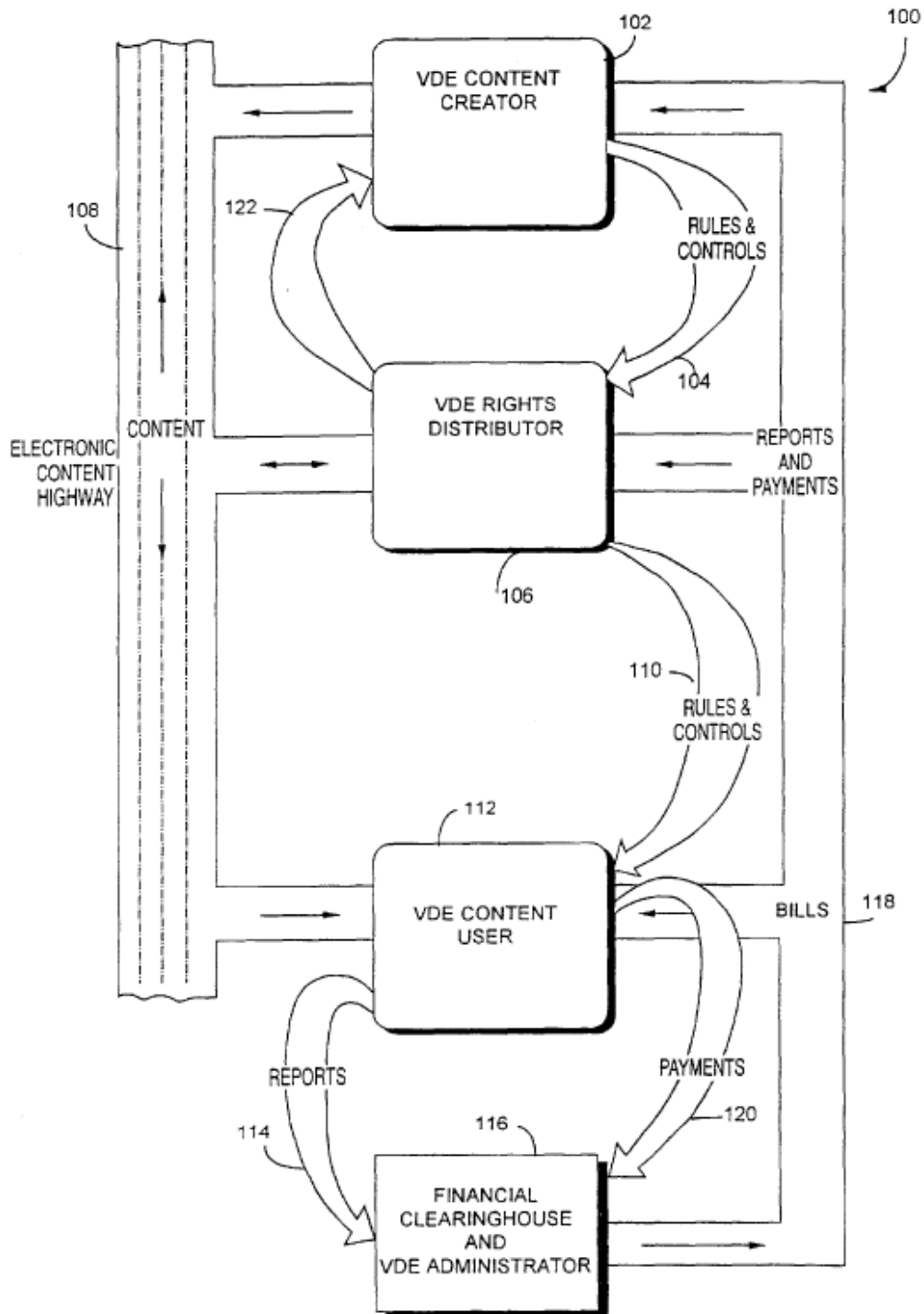
As a related matter, the parties identify *Dolby Laboratories, Inc. v. Intertrust Corp.*, No. 3:19-cv-03371 (N.D. Cal. filed June 13, 2019) (“California Action”). The parties also identify the following three cases in the Eastern District of Texas: *Intertrust Technologies Corp. v. AMC Entertainment Holdings, Inc.*, No. 2:19-cv-00265 (E.D. Tex. filed Aug. 7, 2019); *Intertrust Technologies Corp. v. Cinemark Holdings, Inc.*, No. 2:19-cv-00266 (E.D. Tex. filed Aug. 7, 2019); *Intertrust Technologies Corp. v. Regal Entertainment Group*, No. 2:19-cv-00267 (E.D. Tex. filed Aug. 7, 2019) (collectively, “Texas Actions”). Pet. 3; Paper 18, 2.

B. THE '158 PATENT (EX. 1001)

According to the '158 patent, one “problem for electronic content providers is extending their ability to control the use of proprietary information” so they can “limit use to authorized activities and amounts.” Ex. 1001, 2:41–44. The '158 patent describes techniques for allowing electronic content providers to control their protected information with a “‘virtual distribution environment’ (called ‘VDE’ . . .) that secures, administers, and audits electronic information use.” *Id.* at 2:29–31.

Figure 2, reproduced below, illustrates how a VDE “may be used to provide a ‘chain of handling and control’ for distributing content.” Ex. 1001, 54:4–6.

FIG. 2



As shown above in Figure 2, VDE content creator 102 creates digital content and “may also specify ‘rules and controls’ for distributing the content,” such as “who has permission to distribute the rights to use content, and how many

users are allowed to use the content.” Ex. 1001, 54:10–14. Arrow 104 illustrates how VDE content creator 102 may send these rules and controls to VDE rights distributor 106, who may “generate[] her own ‘rules and controls’ that relate to usage of the content,” such as “what a user can and can’t do with the content and how much it costs.” *Id.* at 54:22–25. VDE rights distributor 106 may, likewise, send its rules and controls to VDE content user 112 (via arrow 110), who uses the content according to all of the above rules and controls. *See id.* at 54:29–33.

The VDE “prevents use of protected information except as permitted by the ‘rules and controls’ (control information)” established for the VDE. Ex. 1001, 55:2–4; *see also id.* at Fig. 2. The “rules and controls may travel with the content they apply to,” or the VDE may “allow[] ‘rules and controls’ to be delivered separately from content.” Ex. 1001, 56:4–7; *see id.* at 54:17–19 (Rules and controls may be sent “over an electronic highway 108 (or by some other path such as an optical disk sent by a delivery service such as U.S. mail).”); *id.* at 56:5–7 (“The content can be distributed over the same or different path used to send the ‘rules and controls.’”). This allows the content distributor to control use of their protected information after its delivery, because “no one can use or access protected content without ‘permission’ from corresponding ‘rules and controls.’” *Id.* at 56:7–10. In the embodiment of Figure 2, the content is shown being sent over electronic content highway 108.

Each participant in the VDE may have a secure electronic appliance (such as a computer) to communicate with other such appliances over electronic content highway 108. Ex. 1001, 58:9–12. One portion of this electronic appliance is a secure processing unit (“SPU”), which “stores

important information securely.” *Id.* at 58:12–16. The SPU can perform such roles as “decrypting . . . VDE protected objects,” or “managing encrypted and/or otherwise secured communication (such as by employing authentication and/or error-correction validation of information).” *Id.* at 61:64–62:1. The SPU “may also perform secure data management processes including governing usage of, auditing of, and where appropriate, payment for VDE objects.” *Id.* at 62:1–4.

An example of an SPU is shown in Figure 6, reproduced below:

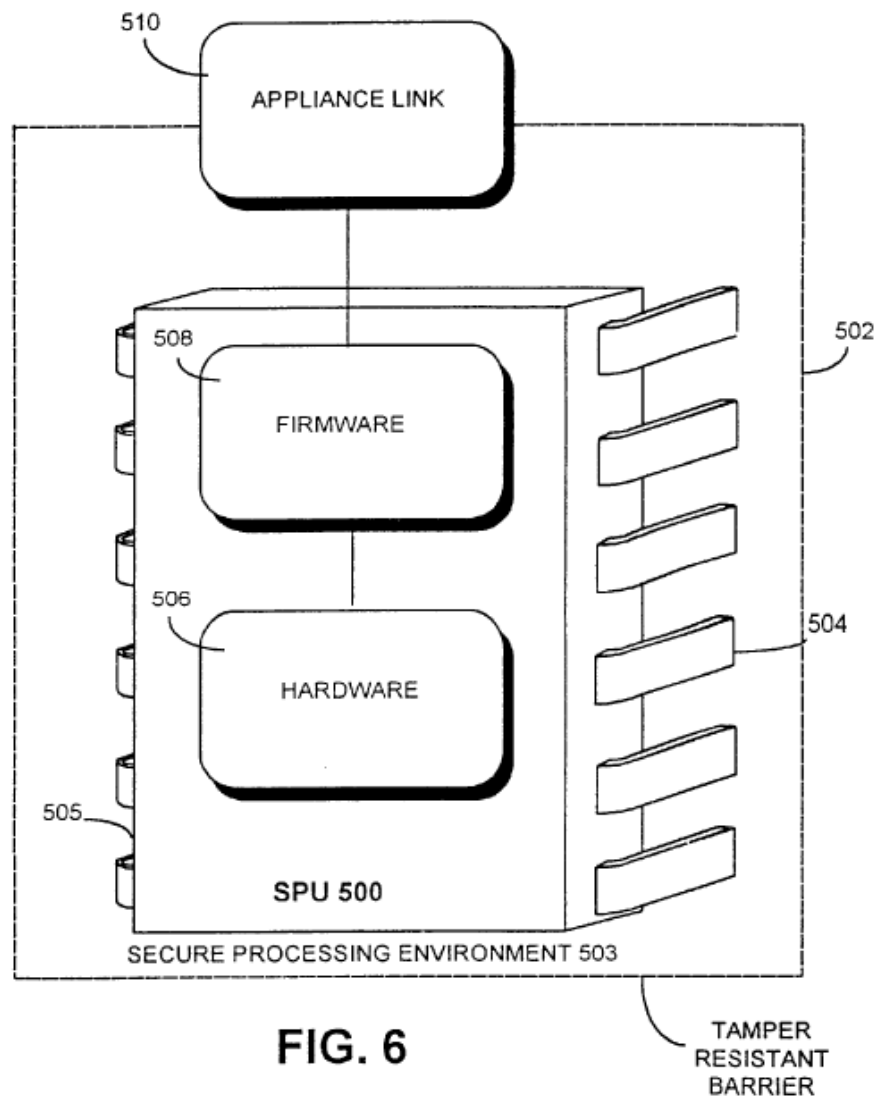


Figure 6, above, depicts SPU 500, which “is enclosed within and protected by a ‘tamper resistant security barrier’ 502” that “separates the secure environment 503 from the rest of the world.” Ex. 1001, 58:18–20. For example, tamper resistant barrier 502 can be “formed by security features such as ‘encryption,’ and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected.” *Id.* at 58:25–29. “Part of this security barrier 502 is formed by a plastic or other package in which an SPU ‘die’ is encased,” which impedes tampering “[b]ecause the processing occurring within, and information stored by, SPU 500 are not easily accessible to the outside world,” since all signals must “cross barrier 502 through a secure, controlled path.” *Id.* at 62:21–27.

The ’158 patent claims a priority date of February 13, 1995, which Petitioner Dolby does not contest in this proceeding. *See* Pet. 5 & n.1; *see also* Ex. 1001, code (63), 1:16.

C. CHALLENGED CLAIM AND ASSERTED GROUNDS OF
UNPATENTABILITY

Claim 4, the sole challenged claim, is as follows:

4. A method utilizing an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method, the method comprising:
 - [a] receiving, at the electronic appliance, an electronic content item, the electronic content item being encrypted at least in part;
 - [b] storing the electronic content item in memory of the electronic appliance;

- [c] receiving, at the electronic appliance, independently from the electronic content item via separate delivery and protected separately from the electronic content item, a rule specifying one or more permitted uses of the electronic content item;
- [d] receiving, at the electronic appliance, a request to use the electronic content item;
- [e] determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule; and
- [f] using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a secure processing unit contained in the electronic appliance.

Ex. 1001, 314:18–40 (Dolby’s reference letters added).

Dolby argues two grounds for *inter partes* review, as summarized in the following table:

Claim Challenged	35 U.S.C. §	Reference(s)/Basis
4	103(a) ¹	Narasimhalu, ² Chorley ³
4	103(a)	Katznelson, ⁴ Chorley

Pet. 7–8.

¹ 35 U.S.C. § 103(a) (2006), *amended by* Leahy–Smith America Invents Act, Pub. L. No. 112-29 § 103, sec. (n)(1), 125 Stat. 284, 287, 293 (2011) (effective Mar. 16, 2013). The 2006 version of § 103 applies because the effective priority date of the ’158 patent is before the effective date of the AIA amendments. *See supra* part II.B.

² Narasimhalu et al., US 5,499,298 (issued Mar. 12, 1996) (Ex. 1004).

³ Chorley et al., US 4,634,807 (issued Jan. 6, 1987) (Ex. 1006).

⁴ Katznelson, US 5,010,571 (issued Apr. 23, 1991) (Ex. 1005).

D. DECLARATORY TESTIMONY

For its Petition and Reply, Dolby relies on the declaration of John R. Black, Jr., Ph.D. Ex. 1002. For its Response and Sur-reply, Intertrust relies on the declaration of Dr. Markus Jakobsson. Ex. 2024. We find both witnesses qualified, based on their education and experience, to offer expert opinions on the subject matter of their respective declarations. *See* Fed. R. Evid. 702(a); *see* Ex. 1002 ¶¶ 4–8, App’x A; Ex. 2024 ¶¶ 4–16, App’x A.

Dolby also submits a declaration by Crena Pacheco (Ex. 1027) authenticating Exhibits 1010–1017, and 1019–1022, and a declaration by Jonathan Bradford (Ex. 1052) authenticating Exhibits 1028–1051. Intertrust does not challenge the authenticity of these exhibits.

III. GROUNDS OF THE PETITION

For the reasons below, we determine that Dolby has shown, by a preponderance of the evidence, that claim 4 of the ’158 patent is unpatentable under § 103(a). Before analyzing the Petition’s asserted grounds in detail, we address two matters that will underlie our analysis: the level of ordinary skill in the art, and the construction we will apply to the claim terms.

A. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the pertinent art at the time of the invention is relevant to how we construe the patent claims. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). It is also one of the factual considerations relevant to obviousness, *see Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966), and it is relevant when

considering whether a reference anticipates a claimed invention, *see In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

To assess the level of ordinary skill, we construct a hypothetical “person of ordinary skill in the art,” from whose vantage point we assess obviousness and claim interpretation. *See In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). This legal construct “presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan.” *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Relying on Dr. Black’s testimony, Dolby argues that a person of ordinary skill in the art “would have been a person who has had a minimum of a bachelor of science degree in computer science, computer engineering, or a related field, and approximately two years of professional experience or equivalent study in network and system security,” and “[a]dditional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.” Pet. 14–15 (citing Ex. 1002 ¶¶ 25–30).

Citing Dr. Jakobsson’s testimony, Intertrust argues that a person of ordinary skill in the art would have had “a Bachelor of Science degree in electrical engineering and/or computer science, and *three years* of work or research experience in the fields of secure transactions and encryption, or a Master’s degree in electrical engineering and/or computer science and two years of work or research experience in related fields.” PO Resp. 12 (citing Ex. 2024 ¶ 19).

Thus, Intertrust argues for a somewhat higher level of ordinary skill in the art than Dolby, with either one additional year of work experience (three years versus two years) or a higher degree (a master’s degree versus a

bachelor's degree). The parties also describe the relevant work experience slightly differently, with Dolby describing the field as “network and system security,” while Intertrust describes work experience of a more specialized nature: “secure transactions and encryption.” Pet. 14; PO Resp. 12.

However, Dr. Jakobsson states that “[t]he opinions set forth in [his declaration] would be the same under either [his] or Dr. Black’s proposal.” Ex. 2024 ¶ 20.

We adopt Dolby’s proposed articulation of a slightly lower level of ordinary skill in the art, because it is consistent with the level of technical expertise assumed by the ’158 patent disclosure and the asserted prior art references. Our analysis would be the same under either party’s proposed level of ordinary skill, and Intertrust would not benefit, in our analysis, from its proposed higher level of ordinary skill.

B. CLAIM CONSTRUCTION

In an *inter partes* review, we construe a patent 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). This includes “construing 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 ordinary and customary meaning of a claim term “is its meaning to the ordinary artisan after reading the entire patent,” and “as of the effective filing date of the patent application.” *Phillips*, 415 F.3d at 1313, 1321. We also consider “[a]ny prior claim construction determination concerning a term of the claim

in a civil action . . . that is timely made of record” in this proceeding. 37 C.F.R. § 42.100(b) (2020).

Dolby argues that we should construe the terms “secure processing unit” and “receiving . . . independently . . . via separate delivery.” Pet. 15–16. Intertrust contends that we should also construe the term “rule.” *See* PO Resp. 13–21. We address each of these terms below.

1. “secure processing unit (SPU)”

In its Petition, Dolby proposes that we construe the term “secure processing unit” (“SPU”) to mean “processing circuitry that functions in a self-contained, trusted computing environment.” Pet. 15 (citing Ex. 1002 ¶¶ 22–24, 60–61). Dolby contends that this is consistent with examples in the ’158 patent in which SPUs “execute processes in self-contained trusted environments” and may include “a tamper-resistant housing, a processor, and memory storing a cryptographic key.” Pet. 16 (citing Ex. 1001, 47:62–48:9, 48:10–56, 58:8–55, 61:60–70:55, 77:54–57, 313:20–25).

In its Response, Intertrust argues that we should adopt the court’s construction in the Texas Actions, which is “processing unit that makes information and processes resistant to unauthorized use.” PO Resp. 13 (citing Ex. 2007, 12–17). Dolby agreed with this construction in its Reply, noting that this is also the same construction adopted in the California Action. Pet. Reply 1 (citing Ex. 1053, 20–23).

We agree with the Texas court’s reasoning, and adopt the same construction now agreed by the parties: “processing unit that makes information and processes resistant to unauthorized use.” *See* Ex. 2007, 12–17.

2. “receiving . . . independently . . . via separate delivery”

In this proceeding and in the California Action, Dolby proposed that “receiving . . . independently . . . via separate delivery” means “receiving via delivery at a different time, over a different path, or from a different source.” Pet. 16 (citing Ex. 1002 ¶¶ 22–24, 62–63); Ex. 1053, 16. In support, Dolby argues that the ’158 patent includes examples of delivery at different times, over different paths, or by different parties. Pet. 16 (citing Ex. 1001, 28:63–65, 41:30, 82:3–11, 127:12–18).

Intertrust notes that, after Dolby filed its Petition, the court in the Texas Actions (to which Dolby is not a party) adopted the parties’ agreed construction of “receiving . . . independently . . . via separate delivery” as meaning “receiving through a different path.” PO Resp. 14 (citing Ex. 2001, 1; Ex. 2007, 12). Intertrust proposes that we adopt the agreed construction from the Texas Actions, because the meaning of the term was narrowed during prosecution of the ’158 patent. *Id.* at 14–18. According to Intertrust, the Examiner rejected, as anticipated, the original wording of what is now claim 4 that specified that the rule was received “independently from the electronic content item.” *Id.* at 16 (emphasis omitted) (citing Ex. 1003, 1122–27); *see* Ex. 1003, 795 (claim 8). The Examiner concluded that the claim language “receiving . . . independently” failed to capture “the implicitly alleged limitation” that the applicant was arguing, “such as ‘the electronic rule and electronic content are *transmitted via two independent (or separate) paths*’ (or *not transmitted within the same package at one time*).” PO Resp. 16 (quoting Ex. 1003, 1123). According to Intertrust, “[t]he Examiner subsequently requested a further amendment specifying ‘via separate delivery’ in order ‘to place the application in condition for

allowance,” and the applicant agreed to the amendment. *Id.* (citing Ex. 1003, 1184–88; Ex. 2024 ¶ 62).

Intertrust argues that “[s]ince the specification makes clear that ‘receiving . . . independently’ means delivered ‘at a different time, over a different path, and/or by a different party,’ the addition of the ‘via separate delivery’ language ‘narrows the scope of claim 4 to require ‘receiving through a different path.’” PO Resp. 16–17 (emphasis omitted) (citing Ex. 1001, 127:12–18). Intertrust points to a similar amendment in the prosecution history of U.S. Patent No. 8,191,157 (a patent in the same family) as further support. *See id.* at 17–18.

Intertrust made similar arguments in the California Action, and likewise proposed that the district court adopt the construction from the Texas Actions. *See* Ex. 1053, 16–18. The California court disagreed, and adopted Dolby’s proposed construction (the same construction Dolby proposes here). *See id.* at 16–20. According to the California court, Dolby’s “proposed construction has the virtue of being rooted in ‘the actual claim language adopted by the patentee,’” which “sets a high bar for Intertrust to clear in arguing for an alternative construction,” which Intertrust failed to do. *Id.* at 19 (quoting Dolby’s responsive brief in the California Action). The court also stated that “the defendants’ stipulation in [the Texas Action] to the construction Intertrust proposes is mostly irrelevant here, as the court in that case did not offer any analysis on the issue.” *Id.*

We agree with the California court, for the reasons set forth in the court’s Claim Construction Order. Ex. 1053, 19–20. We also find persuasive Dolby’s argument, in this case, that “[i]f Applicant’s intention was to claim *only* a different path *and exclude everything else* (times, parties, and any

other reasonable understanding of delivery), this intention is nowhere explained, let alone clearly expressed as a disclaimer” during prosecution. Pet. Reply 2. Thus, we adopt the construction adopted in the California Action: “receiving via delivery at a different time, over a different path, or from a different source.” Ex. 1053, 20.

3. “*rule*”

Intertrust argues that we should construe the term “rule” according to its construction in the Texas Actions, which was “information and/or programming controlling operations on or use of resources.” PO Resp. 19 (citing Ex. 2007, 40).

In its Reply, Dolby agrees with the Texas court’s construction “if construction is necessary.” *See* Pet. Reply 4–5. Dolby notes, however, that the court in the California Action has adopted a similar construction: “information and/or programming controlling operations on or use of a digital file or electronic item.” *Id.* at 5 n.1 (citing Ex. 1053, 8–11). We consider this construction to be the same as the Texas court’s construction, except that in response to further arguments by Dolby and Intertrust, the California court further clarified that the “resources” falling within the scope of this claim term are specifically “a digital file or electronic item.” *See* Ex. 1053, 8–11. Here, neither Dolby nor Intertrust contest that the controlled “resources” are specifically a digital file or electronic item. *See, e.g.*, Pet. Reply 5–6; PO Sur-reply 12–20.

We agree with the California court’s reasoning, and apply the same construction: “information and/or programming controlling operations on or use of a digital file or electronic content item.” Ex. 1053 8–11.

C. GROUND BASED ON NARASIMHALU AND CHORLEY

For its first ground, Dolby alleges that claim 4 is unpatentable under § 103(a) as obvious over Narasimhalu in view of Chorley. Pet. 8, 17–42.

A claim is unpatentable under § 103(a) for obviousness 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). For a combination of known elements that are not explicitly found together in the prior art, we consider “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *Id.* at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). A successful petition must “articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016) (citing *KSR*, 550 U.S. at 418); *see also* 35 U.S.C. § 322(a)(3); 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4) (2020).

We base our obviousness inquiry on factual considerations 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 skill in the art, and (4) any objective indicia of obviousness or non-obviousness that may be in evidence. *See Graham*, 383 U.S. at 17–18.

Based on these factors, Dolby has shown that claim 4 is unpatentable under 35 U.S.C. § 103(a) as obvious over Narasimhalu in view of Chorley. We present our findings and conclusions below.

1. Overview of Narasimhalu

Narasimhalu generally relates to “controlling the dissemination of digital information” using “a tamper-proof controlled information access device.” Ex. 1004, code (57). The general model for disseminating information is shown in Figure 1, reproduced below. *Id.* at 4:47–48.

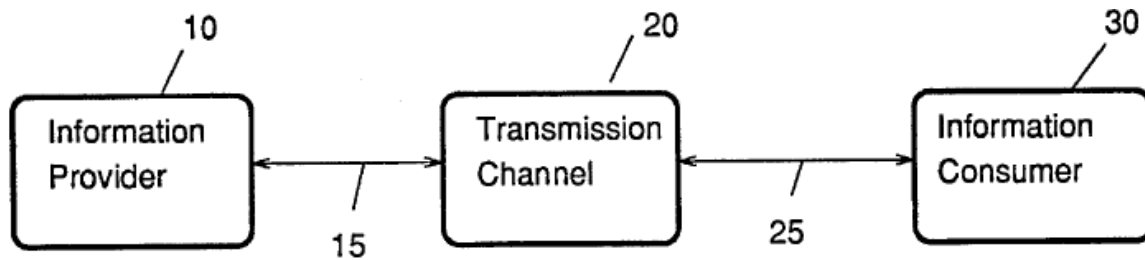


Figure 1, above, depicts information provider 10, which communicates to information consumer 30 over transmission channel 20 via paths 15 and 25. Ex. 1004, 4:48–54. Information consumer 30 represents “one or more end users of information.” *Id.* at 4:58–60.

Information consumer 30 has a device, such as a computer, to access the information in the distributed medium. Ex. 1004, 6:47–49. Narasimhalu describes two embodiments of this access device. The first embodiment, shown in Figure 3, reproduced below, is part of an “off-line scheme” for accessing the electronic information, in the case that transmission channel 20 is a “non-volatile storage medium.” *Id.* at 5:26–31.

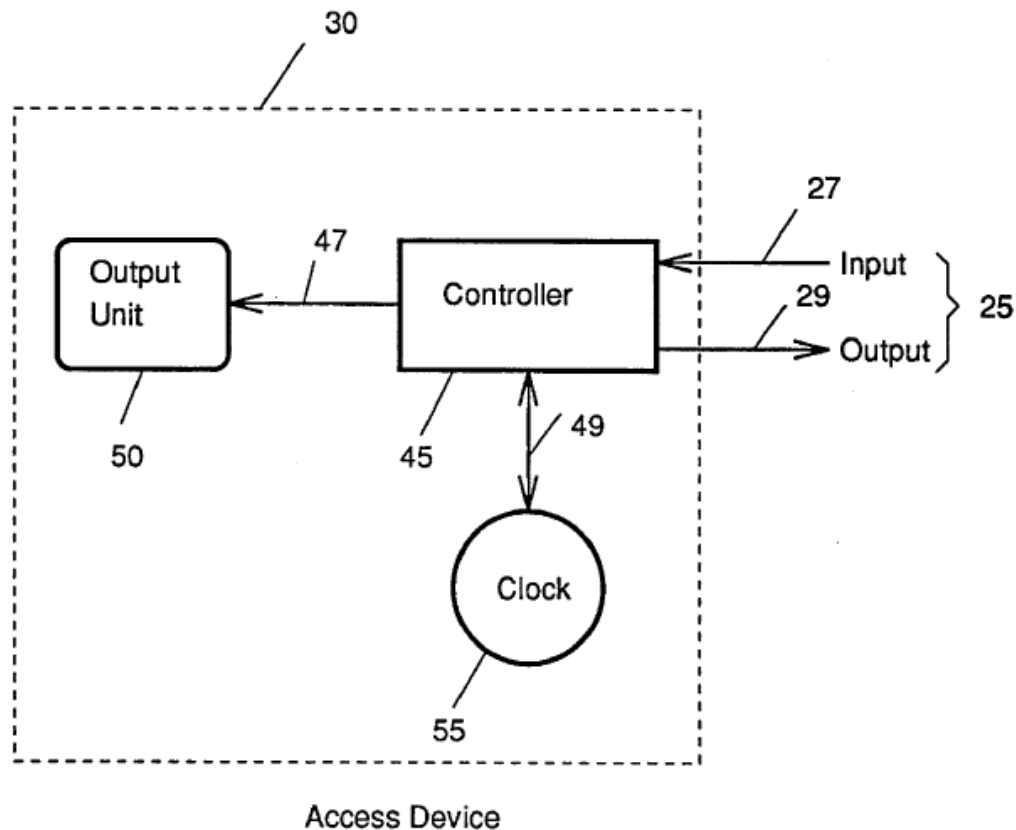


Figure 3

Figure 3, shown above, depicts the “minimum enhancements” to a “device, for example a computer,” to access the electronic content. *See* Ex. 1004, 6:47–50. The device includes controller 45 “coupled as its input to an information input channel 27 for receiving disseminated information from the read device (not shown)” of storage medium 20, and also “coupled at one of its outputs to an information output channel 29 for transmitting re-encrypted information to the write device (not shown)” of storage medium 20. *Id.* at 6:50–57. Controller 45 is also coupled via link 49 to a clock, and via link 47 to output unit 50, which “could be a display unit” or “a device for distributing controlled information to other information consumers.” *Id.* at 6:61–7:3.

The second embodiment of the access device is part of “an online scheme” for accessing the electronic content, in the case that transmission channel 20 is a communication link (such as a computer network or telephone lines) between Information Provider 10 and Information Consumer 30. Ex. 1004, 8:30–35, 8:38–40. An example is shown in Figure 6, reproduced below.

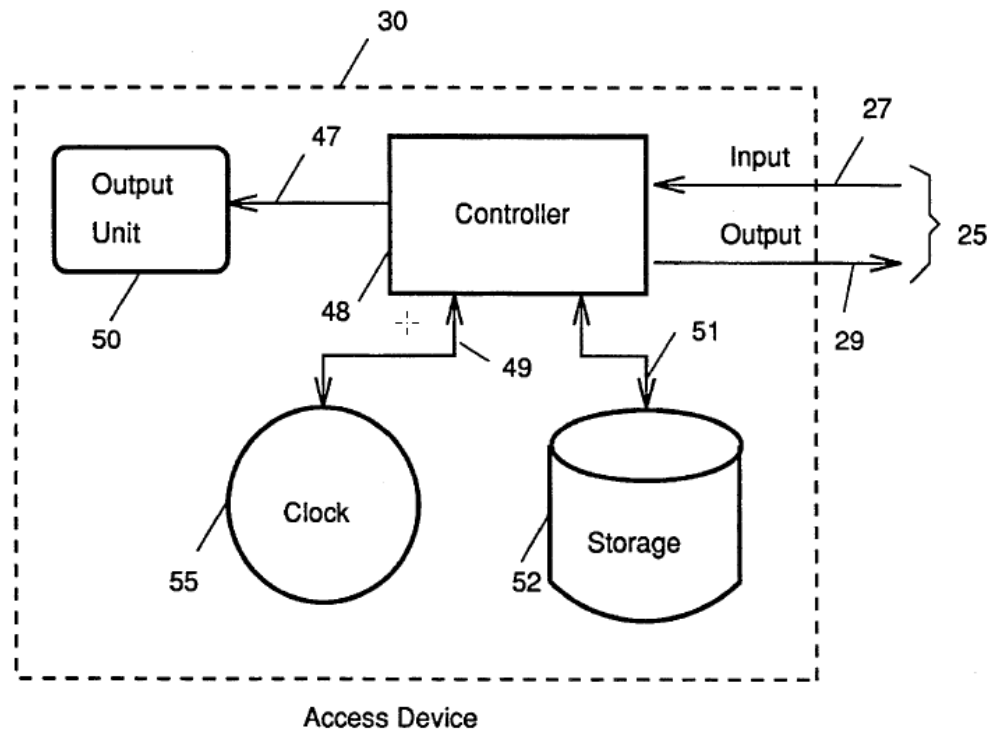
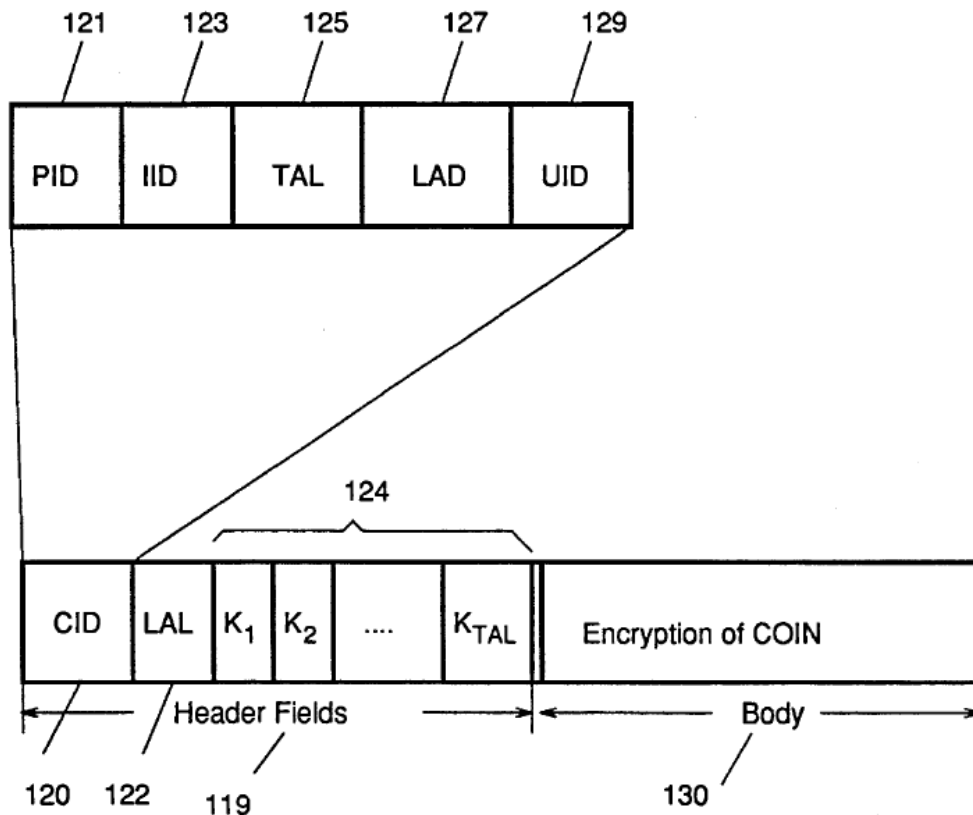


Figure 6

Figure 6, above, depicts an access device for use in an online scheme, “modeling the Information Consumer 30.” Ex. 1004, 8:38–40. “Controlled information from the transmission channel 20 is presented to the Information Consumer 30 over an input channel 27 which is coupled to a Controller 48.” *Id.* at 8:40–42. “Controller 48 can be implemented either in hardware or by a general purpose processor with proper software.” *Id.* at 8:44–46. It controls the flow of information through input channel 27 and output channel 29. *Id.*

at 8:40–42, 8:53–55. Like the first embodiment in Figure 3, the access device of Figure 6 includes output unit 50 and clock 55, but it also includes memory storage 52. *See id.* at 8:46–53. “Preferably, the various channels coupled to the Controllers 48 are tamper-proof. This will make it impossible for users to tap into the clear channel 47, to access the Controller 48, to alter the value of the memory storage 52, or to change the value of the clock 55.” *Id.* at 8:55–59.

As part of the second (Figure 6) embodiment, information provider 10 disseminates the protected information to information consumer 30’s access device through a sealed “controlled information” (“COIN”). Ex. 1004, 5:22–26. Figure 7A of Narasimhalu, reproduced below, illustrates a possible format of the COIN. *Id.* at 3:28–30, 9:15–17.



As shown above in Figure 7A, the COIN includes header 119 and body 130 of encrypted information. Ex. 1004, 9:52–53. Header 119 further includes the following three fields: (1) identification of a contract of information dissemination (“CID”) 120 that includes, among other things, total number of legal accesses to the COIN (“TAL”) and identification of the device on which the COIN can be accessed legally (“LAD”); (2) identification of the number of legal accesses left (“LAL”) 122; and (3) keys 124 used to decrypt body 130 and further encrypt the COIN to form a new COIN. *Id.* at 9:22–26, 9:57–61.

Narasimhalu discloses that, in order to access the information stored in the COIN, “[a] user presents the Sealed-COIN together with a ticket to access [the] device.” Ex. 1004, 9:11–12. This ticket is called a “[s]ealed [o]pener” or “[o]pener.” *Id.* at 9:12–13. A possible format for an opener is shown in Figure 7B, reproduced below.

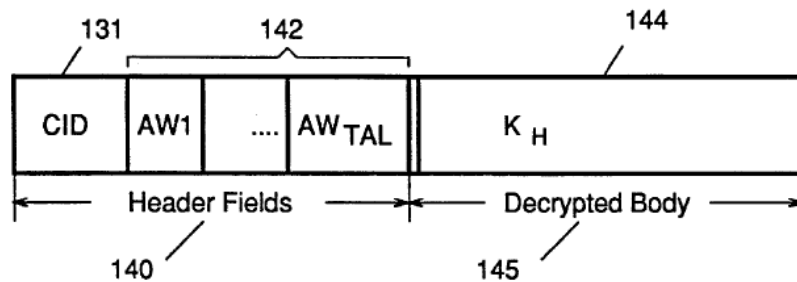


Figure 7B

Figure 7B, above, depicts an opener comprising header 140 and body 145. Ex. 1004, 9:62–63. Header 140 comprises CID 131 (the same as CID 120 in the associated Sealed COIN) and access windows (AWs) 142, which indicate times during which a user is allowed to access the associated COIN. *Id.* at 9:35–36, 9:63–67. Body 145 contains decryption key K_H for decrypting header 119 of the associated COIN. *Id.* at 9:67–10:2.

A flowchart of the process by which information consumer 30 obtains and uses a COIN is shown in Figure 10, reproduced below. Ex. 1004, 3:43–45, 10:11–13.

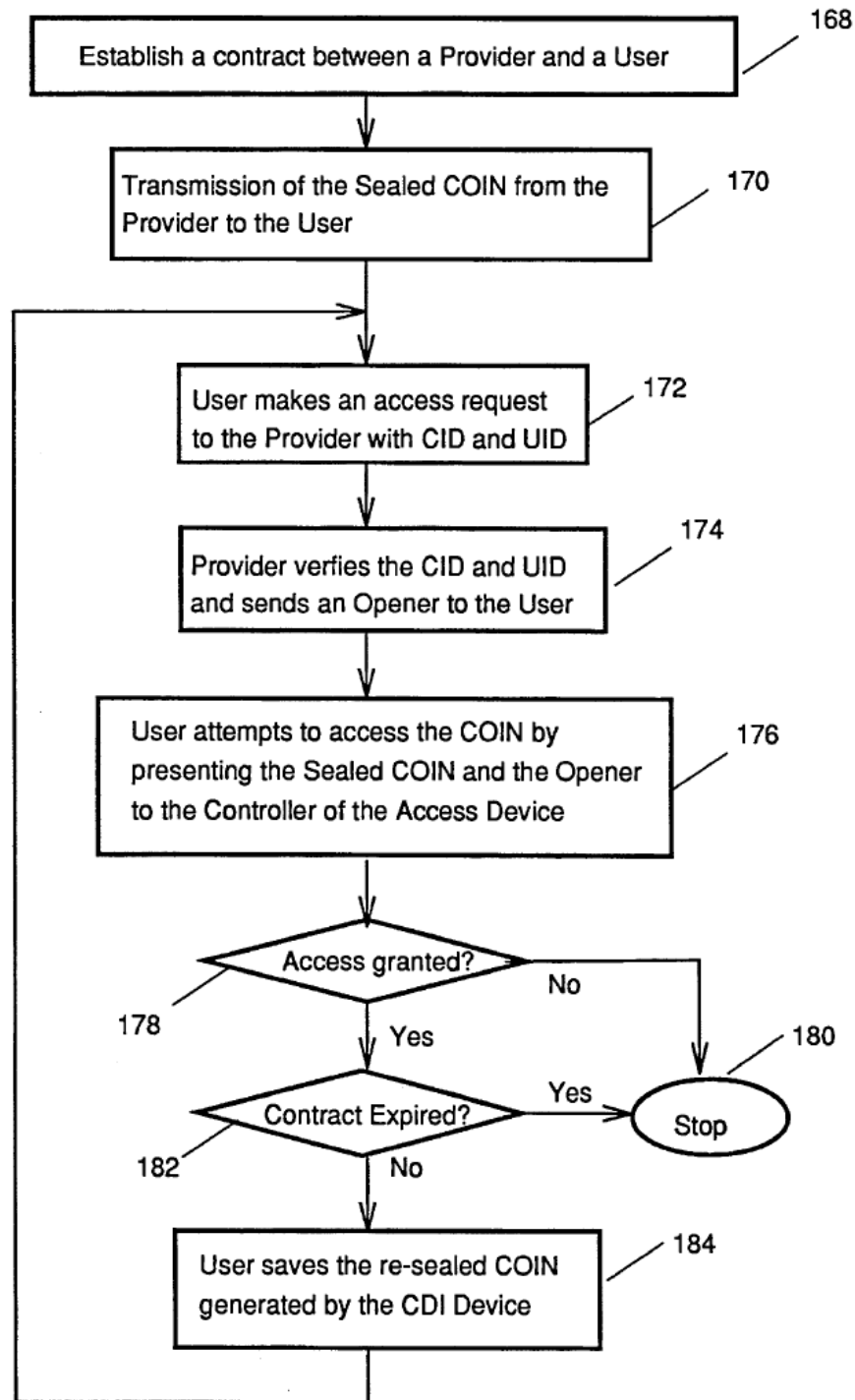


Figure 10

Figure 10, above, illustrates the following steps: (1) information provider 10 and information consumer 30 establish a contract between each other (step 168); (2) information provider 10 generates a COIN and transmits it to information consumer 30 (step 170); (3) information consumer 30 sends a request to information provider 10 to access the controlled information within the sealed COIN (step 172); (4) after verifying the request, Information Provider 10 generates and transmits an opener to information consumer 30 (step 174); (5) information consumer 30 attempts to access the COIN by presenting the COIN and the opener to controller 48 of information consumer 30's access device (step 176); and (6) controller 48 checks to see if access should be granted (step 178) and, if access is granted, outputs the COIN. Ex. 1004, 10:11–46.

2. *Overview of Chorley*

Chorley, titled “Software Protection Device” is directed to an apparatus and method of protecting software. Ex. 1006, codes (54), (57), 1:4–5. Chorley describes the apparatus as “a software protection device (SPD).” *Id.* at 2:9–11. An SPD is illustrated in Figure 1, reproduced below:

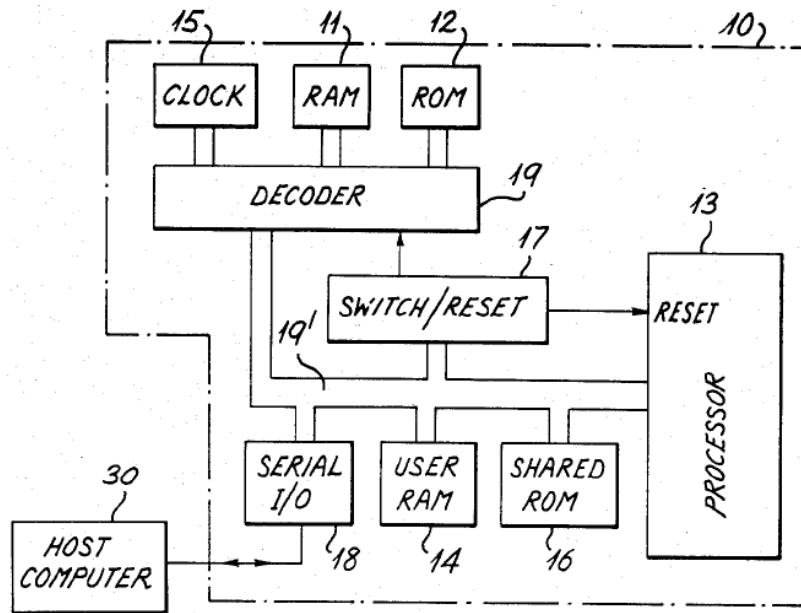


Fig. 1

As shown in Figure 1, above, SPD 10 comprises RAM 11, which stores a user's cryptographic keys, and processor 13. Ex. 1006, 4:5–37. SPD 10 also includes user RAM 14 which stores protected software both before and after it is decrypted, and this software is eventually run on processor 13. *See id.* at 4:32–34, 5:28–30, 5:38–41. SPD 10 may be integral with or independent from host computer 30. *Id.* at 5:35–39.

To decrypt electronic content, the content is loaded into host computer 30, transmitted to SPD 10, and stored in the SPD's RAM 14. Ex. 1006, 5:28–32. An encrypted key is retrieved from RAM 14, decrypted, placed in RAM 11, and used to decrypt the electronic content. *Id.* at 5:35–39. The tamper-resistant housing of SPD 10 may include a plurality of detectors arranged in layers, each detector being designed to sense a particular mechanical, electrical, or electromagnetic attack. *Id.* at 6:12–15. When tripped, each detector triggers an alarm and a sequence of instructions for erasing sensitive information from RAM 11. *Id.* at 6:15–18.

3. *Motivation to combine Narasimhalu and Chorley*

Dolby relies on Chorley to provide an explicit disclosure of storing encrypted electronic content and encryption keys inside a secure electronic appliance, as required in limitations 4b and 4f, respectively. *See* Pet. 33–34, 40–42. Dolby contends that a person of ordinary skill in the art “would have been motivated to implement [Chorley’s] techniques because they represent conventional and routine techniques used to practice computer-based systems and methods in the art.” Pet. 26 (citing Ex. 1002 ¶¶ 85–93); *see also* Pet. 29 (citing Ex. 1002 ¶ 92). According to Dolby, the advantage of storing the electronic content and keys within the tamper-resistant housing is that they “are protected . . . from access by a user or a connected host computer.” Pet. 28 (citing Ex. 1006, 2:41–51, 6:7–11; Ex. 1002 ¶¶ 42–46, 90). Dolby also argues that, because Narasimhalu’s secure device needs to access the content multiple times, “storing the content, the keys, and the program for accessing the content would have ensured that the content was available to the user at a later time.” Pet. 29 (citing Ex. 1004, 4:65–5:1, 5:35–41, 8:19–23, 8:64–9:3; Ex. 1002 ¶¶ 33, 91).

In addition, Dolby contends that a person of ordinary skill in the art would have had a reasonable expectation of success in applying Chorley’s teachings of storing the content and keys in the secure device, because Narasimhalu’s device already contains memory storage 52, so using that memory the way Chorley uses RAM 11 and RAM 14 would have been “conventional storage operations [that] would have been well within the skill of a [person of ordinary skill in the art].” Pet. 29 (citing Ex. 1002 ¶¶ 33, 93).

Intertrust does not contest Dolby’s motivation to combine. *See* PO Resp. 21–39; *see also id.* at 38–39 (discussing Dolby’s contentions

regarding limitation 4f, but not challenging the motivation to combine Narasimhalu with Chorley). We find Dolby's arguments persuasive for the reasons given in the Petition.

4. *Limitations of Claim 4*

Below, we address Dolby's arguments as to the preamble and each limitation of claim 4.

(a) Preamble

The preamble recites “[a] method of utilizing an electronic appliance comprising a processor and a memory encoded with program instructions that, when executed by the processor, cause the processor to perform the method.” Ex. 1001, 314:18–21. Dolby does not assert that the preamble is limiting, but argues that Narasimhalu discloses such a method operating on an electronic appliance. Pet. 30–31 & n.5 (citing Ex. 1004, 4:23–25, 4:31–42; Ex. 1002 ¶¶ 94–96, 119).

Intertrust does not contest Dolby's assertions regarding the preamble. We find Dolby's argument persuasive, so we do not need to decide whether the preamble is limiting for this decision. *See 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.’”).

(b) Limitation 4a

Limitation 4a recites “receiving, at the electronic appliance, an electronic content item, the electronic content item being encrypted at least in part.” Ex. 1001, 314:22–24. Dolby points to passages in Narasimhalu describing receiving an encrypted electronic content item (the COIN)

through a computer network. Pet. 31–32 (citing Ex. 1004, 4:47–57, 5:35–43, 7:13–27, 8:38–46, 9:7–11, 9:53–57, 10:19–22; Ex. 1002 ¶¶ 97–99, 119).

Intertrust does not contest Dolby’s contentions regarding limitation 4b. We find Dolby’s arguments and supporting testimonial evidence persuasive.

(c) Limitation 4b

Limitation 4b recites “storing the electronic content item in memory of the electronic appliance.” Ex. 1001, 314:25–26. Dolby argues that Narasimhalu’s electronic appliance includes a memory. Pet. 32–33 (citing Ex. 1004, 3:65–68, 8:38–42; Ex. 1002 ¶¶ 100–101). Dolby also contends that Chorley’s device includes user RAM 14 into which the electronic content is stored. Pet. 33–34 (citing Ex. 1006, 3:51–55, 5:28–30, 5:51–55; Ex. 1002 ¶ 119). Dolby argues that a person of ordinary skill in the art would have modified Narasimhalu, based on Chorley’s disclosure, to store the electronic content in Narasimhalu’s electronic appliance, because “[s]toring information provides local access to data for processing,” and also, “where Narasimhalu discloses accessing electronic content multiple times, [this] provides long-term storage for future access attempts.” Pet. 33 (citing Ex. 1002 ¶¶ 90–93).

Intertrust does not contest Dolby’s contentions regarding limitation 4b. We find Dolby’s arguments and supporting testimonial evidence persuasive.

(d) Limitation 4c

Limitation 4c recites “receiving, at the electronic appliance, independently from the electronic content item via separate delivery and

protected separately from the electronic content item, a rule specifying one or more permitted uses of the electronic content item.” Ex. 1001, 314:27–31. Dolby argues that Narasimhalu discloses this limitation. Pet. 34–36 (citing Ex. 1002 ¶¶ 104–108, 119).

In particular, Dolby identifies the “electronic content item” in Narasimhalu as the COIN, and the “rule” as the COIN’s associated opener. *See* Pet. 34. According to Dolby, the opener contains “rules specifying permitted uses of the electronic content item,” including the AW, CID, and LAD fields. Pet. 34–35 (citing Ex. 1004, 9:11–15, 9:20–36, 9:37–43, 9:62–67, 11:7–9); *see also id.* at 34–35 n.7 (citing Ex. 1001, 53:21–27, 54:23–26, 55:4–7, 56:26–57:4, 57:38–61; Ex. 1002 ¶¶ 39–41) (comparing these fields to examples of “rules and controls” in the ’158 patent).

Dolby also contends that the opener (the rule) is protected separately from the COIN (the electronic content item) because “the Opener is encrypted using the access device’s public key DPK, while the COIN is encrypted with keys K₁ to K_T.” Pet. 36 (citing Ex. 1004, 9:52–61, 10:52–58, 10:66–11:11). Dolby also contends that the opener (the rule) is received via separate delivery from the COIN (the electronic content) because information consumer 30 receives the COIN earlier (i.e., at a different time) than the opener. Pet. 35–36 (citing Ex. 1004, 10:18–28).

In response, Intertrust disputes two aspects of Dolby’s argument: (1) that Dolby equates Narasimhalu’s access device (i.e., the “electronic appliance”) with information consumer 30; and (2) Dolby’s contention that the electronic appliance receives the COIN and the opener at different times. *See* PO Resp. 21. We address these issues below.

(1) *Whether Narasimhalu's Access Device Is
the Same as Information Consumer 30*

Intertrust argues that Dolby incorrectly identifies the recited “electronic appliance” as Information Consumer 30, which Narasimhalu describes as the end user of information. PO Resp. 22–23 (citing Ex. 1004, 4:57–60, 7:13–17, 10:11–31, Fig. 10; Ex. 1002 ¶¶ 83, 110; Ex. 2024 ¶¶ 71–72). According to Intertrust, “User/Information Consumer 30 and the ‘access device’ are distinctly different and separate from one another,” and a person of ordinary skill in the art “would have understood from Narasimhalu’s teachings that the User/Information Consumer has a personal computer or other electronic system to communicate with the separate access device shown in FIGS. 3 and 6 of Narasimhalu, which is used to decrypt and play the content received in the sealed-COIN.” *Id.* at 23–24 (citing Ex. 1004, 4:51–57, 5:26–31, 6:22–45, 6:47–49, 7:28–29, 7:45–47, 8:3–6, 9:10–13, 10:13–30, Figs. 1, 4, 10; Ex. 2024 ¶¶ 73–74).

As further support, Intertrust argues that (1) “the information consumer presents the sealed-COIN and Opener together to the access device’s controller 45/48 for accessing the COIN,” PO Resp. 24 (citing Ex. 1004, 9:10–13, 10:28–31; Ex. 2024 ¶ 75); (2) “the access device re-seals and outputs the COIN back to the User/Information Consumer on the output channel 29 (via a write device) for saving and future requests,” *id.* at 24–25 (citing Ex. 1004, 6:53–57, 10:13–46, Fig. 10; Ex. 2024 ¶ 76; (3) “the access device’s secret key is ‘unknown to the Information Consumer 30,’” *id.* at 25 (quoting Ex. 1004, 7:28–29) (citing Ex. 1004, 11:21–22; Ex. 2024 ¶ 77; and (4) “the access device includes special purpose hardware, such as a tamper-proof clock 55 and tamper-proof channels 47, that would ordinarily not be

found in a standard personal computer,” *id.* (citing Ex. 1004, 7:3–10; Ex. 2024 ¶ 78).

Intertrust also addresses the fact that there are dashed boxes labeled “30” in Figures 3 and 6 (where “30” otherwise refers to the information consumer), and that Narasimhalu identifies Figure 6 as “an access device modeling the Information Consumer 30.” PO Resp. 25 (quoting Ex. 1004, 8:38–40). Intertrust argues that a person of ordinary skill in the art would have understood that these disclosures are “meant to convey that the User/Information Consumer 30 *uses* the access devices . . . , not that the User/Information Consumer 30 *is* the access device shown in FIGS. 3 and 6.” *Id.* at 25–26 & n.5 (citing Ex. 1004, 4:57–65; Ex. 2026, 70:12–25 (Black deposition); Ex. 2024 ¶ 79).

In its Reply, Dolby argues that references in the ’158 patent to information consumer 30 also refer to the human user’s electronic apparatus, such as disclosed in Figures 3 and 6. *See* Pet. Reply 5–11. Dolby contends that “Narasimhalu describes that operations are performed on devices such as reconfigured general purpose computers or specialized apparatuses.” *Id.* at 6 (citing Ex. 1004, 4:21–23 (“In most cases, in any of the operations described herein . . . , the operations are machine operations.”); *id.* at 4:17–42). According to Dolby, Narasimhalu uses the term “information consumer” to refer to either a person or a device that is the “end user” of information and to convey the idea that the information is “consume[d]” and thereafter no longer exits. *Id.* at 9–10 (citing Ex. 1004, 4:57–65, 8:25–11:62); *see also id.* at 6 (citing Ex. 1004, 4:17–42).

Dolby also notes that Narasimhalu discloses both offline (Figure 3) and online (Figure 6) embodiments, and Dolby distinguishes between the

two embodiments as to their potential need for human intervention. *See* Pet. Reply 6–8. According to Dolby, “[t]he (first) embodiment in Fig. 3 may involve a person performing certain steps—e.g., physically loading a disk containing the Sealed-COIN—since [information provider 10] is not physically at the same location as [information consumer 30] and likely uses an intermediary to load the disk.” *Id.* at 8 (citing Ex. 1004, 7:13–17). Dolby contrasts this with the second embodiment (Figure 6), which “does not require the same because the transmission channel [20] is a computer network. In fact, the person does not, and cannot, act as a transporter of electrical signals over a network the same way they would act as a transporter of a disk mailed from a[n Information] Provider.” *Id.* Thus, Dolby contends that a person of ordinary skill in the art would have understood “that Narasimhalu’s on-line embodiment transmits information to a Consumer computing device over the computer network.” *Id.* at 9.

Dolby also argues that, according to Narasimhalu, an “information consumer” 30 may also be another information provider 10, yet Narasimhalu discloses that an information provider performs computing tasks, and that a person of ordinary skill in the art “would not interpret this disclosure as a human being generating keys and headers of a digital file, or somehow manipulating bits of data by hand using Morse code.” Pet. Reply 10 (citing Ex. 1004, 5:2–15 (“For one skilled in the art, it is obvious that some of [the steps taken by information provider 10] shall be best automated by, for example, implementing them as a special purpose software”), 8:32–37, 10:47–11:11).

In its Sur-reply, Intertrust contends that its argument is not that information consumer 30 is “plugged into a computer network” and

performing all the functions of Narasimhalu's access device, but rather that Narasimhalu discloses two distinct devices, and the human information consumer uses one of the devices to interact with an access device such as that shown in Figure 6. *See* PO Sur-reply 1–2. According to Intertrust, Dolby has not rebutted the evidence that Intertrust pointed to in its Reply, based on Narasimhalu's disclosure, suggesting the existence of two distinct devices. *Id.* at 2.

Based on the evidence of record, we disagree with Intertrust that a person of ordinary skill in the art would have understood that Narasimhalu teaches using a separate device to interact with the access device of Figure 6. Rather, we agree with Dolby that a person of ordinary skill in the art would have understood that the operations described in the Figure 6 embodiment are automated operations by the access device. *See* Pet. Reply 6 (citing Ex. 1004, 4:17–42). As Narasimhalu describes its disclosed embodiments, “the manipulations performed are often referred to in terms such as adding or comparing, which are commonly associated with the mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable.” Ex. 1004, 4:17–21. Thus, according to Narasimhalu, “[i]n most cases, in any of the operations described herein which form part of the present invention, the operations are machine operations.” *Id.* at 4:21–23.

That Narasimhalu sometimes discloses machine operations as if there were a human performing them also explains why Narasimhalu describes Figure 6 as “[t]he architecture of an access device *modeling* the Information Consumer 30,” and why Figures 3 and 6 contain a box labeled “30,” even

though there is computer hardware (obviously nonhuman) inside the box.
Ex. 1004, 8:38–39 (emphasis added); *see also id.* at Figs. 3, 6.

We do not agree with Intertrust that Narasimhalu contains teachings inconsistent with Dolby’s argument. *See* PO Resp. 24–25. Although Narasimhalu discloses that “[a] user presents the Sealed-COIN together with a ticket to the access device in order to access the COIN” (Ex. 1004, 9:10–12; *see also id.* at 10:28–31 (describing this as an action by “the information consumer”)), a person of ordinary skill in the art would have understood, for the reasons discussed above, that this is an automated process by the access device. Intertrust does not point to anything in Narasimhalu reasonably indicating that a second computer is involved in this process.

We do agree with Intertrust that Narasimhalu discloses that the access device can re-seal and output a COIN back through output channel 29. PO Resp. 24 (citing Ex. 1004, 6:53–57,⁵ 10:13–46, Fig. 10). We also agree that an information consumer 30 can re-use that COIN in future accesses. *See* Ex. 1004, 10:39–46. But again, we find persuasive Dolby’s argument that a person of ordinary skill in the art would have understood that these operations are performed in the access device, and Intertrust points to nothing in Narasimhalu reasonably indicating that a second computer is involved.

We also do not find this determination inconsistent with Dolby’s argument that the access device in Figure 6 has its “own” secret key, or that

⁵ This citation refers to the Figure 3 “off-line” embodiment, which Dolby does not rely on. But in this case, the re-sealed COIN is sent via channel 29 “to the write device” (e.g., a disk drive), not to a separate user computer. *See* Ex. 1004, 6:53–57.

(in the Figure 3 embodiment, at least) the information consumer does not know this key. *See* PO Resp. 25 (citing Ex. 1004, 7:28–29, 11:21–22; Ex. 2024 ¶ 77). This simply suggests, as Dolby argues in its Petition, that the access device’s secret key is not available to the human information consumer. *See* Pet. 40 (“[T]he secret key DSK is disclosed as belonging to the Access Device and is unknown to the Information Consumer, so a [person of ordinary skill in the art] would have recognized that it is stored in the Access Device.”).

Finally, we find no indication of a second, distinct computer in Narasimhalu’s teachings that “the access device includes special purpose hardware . . . that would ordinarily not be found in a standard personal computer.” PO Resp. 25 (citing Ex. 1004, 7:3–10; Ex. 2024 ¶ 78). As Dolby persuasively argues, Narasimhalu teaches that the access device can be a modified general purpose computer. *See* Pet. Reply 6 (citing Ex. 1004, 4:17–42, 6:51–57, 8:38–40).

For the above reasons, we disagree with Intertrust that the information consumer 30’s operations in the Figure 6 embodiment should be ascribed to a second, distinct computer rather than Narasimhalu’s access device.

(2) *Whether the Electronic Appliance Receives the COIN and Opener at Different Times*

Intertrust argues that Dolby has failed to show that Narasimhalu’s electronic appliance receives the COIN and opener “via separate delivery” as recited in claim 4. *See* PO Resp. 26–28. Intertrust acknowledges that information provider 10 transmits the COIN to information consumer 30 first, and then transmits the opener at a different time. *See id.* at 26 (citing Ex. 1004, 10:11–28). But according to Intertrust, it is not information

consumer 30's *access device* that receives the COIN and the opener, but a distinct, second device, which the human user then also uses to submit the COIN and the opener, simultaneously, to the access device. *Id.* at 27 (citing Ex. 1004, 9:11–13, 10:28–31). Thus, according to Intertrust, “the access device receives the COIN and Opener at the same time, not at different times.” *Id.* at 27–28 (citing Ex. 2024 ¶¶ 80–81).

Also, Intertrust argues that, in Narasimhalu, the COIN and the opener follow the same path between information provider 10 and information consumer 30, which is through transmission channel 20. PO Resp. 28–29 (citing Ex. 1004, 10:19–31, Fig. 10; Ex. 2024 ¶ 83). Thus, Intertrust contends that Narasimhalu fails to meet Intertrust's proposed construction of “receiving . . . independently . . . via separate delivery” that “requires that the rule be received at the electronic appliance through a different path than that of the content item.” *Id.* at 28 (citing Ex. 2024 ¶ 82).

As we discuss above, Dolby disagrees, in its Reply, with Intertrust's position that information provider 10 transmits the COIN and the opener initially to a second, distinct, computer rather than the access device. *See* Pet. Reply 5–11; *supra* part III.C.4(d)(1).

Intertrust's arguments depend on (1) reading Narasimhalu to imply that operations attributed to information consumer 30 take place on a second computer, distinct from the access device, and (2) applying Intertrust's proposed construction for “receiving . . . independently . . . via separate delivery,” which requires delivery by different paths. As we discuss above, we disagree with Intertrust on both points. *See supra* parts III.C.4(d)(1), III.B.2. We also find Dolby's arguments persuasive, and well founded on the text of Narasimhalu, that the access device receives the COIN and the

opener at different times. In particular, we agree with Dolby that Narasimhalu's Figure 10 clearly discloses that information provider 10 transmits the COIN (step 170) and the opener (step 174) to the "User" at different times, and that since the process is automated, these actions by the "user" take place on the access device itself, and not a separate, distinct computer. Ex. 1004, 10:11–31. To the extent that Dr. Jakobsson's testimony is inconsistent with this conclusion, we find it less credible than Dr. Black's testimony supporting the Petition and the clear teachings of Narasimhalu that Dolby identifies in its Reply.

For the above reasons, we find that Dolby has shown that Narasimhalu discloses limitation 4c.

(e) Limitation 4d

Limitation 4d recites "receiving, at the electronic appliance, a request to use the electronic content item." Ex. 1001, 314:32–33. Dolby maps the recited request to "presenting the COIN and the Opener" to the access device's controller in step 176 of Narasimhalu's Figure 10. *See* Pet. 36–37; Pet. Reply 13.⁶ Dolby notes that, at step 176, Figure 10 states that by presenting the COIN and the opener to controller 48, the "[u]ser attempts to access the COIN." Pet. 37 (emphasis omitted) (quoting Ex. 1004, Fig. 10). Dolby also argues that a person of ordinary skill in the art "would have recognized that, because the requests are made by users at the Information Consumer 30 (which includes the Controller of the Access Device) . . . , the

⁶ Alternatively, Dolby maps the recited request to the user's "access request" to use the COIN (step 172 in Figure 10). Pet. 36–38 (citing Ex. 1004, 9:13–31, 10:22–31, 11:13–15, Fig. 10). Because we find Dolby's other argument persuasive, we need not address this alternative argument.

request is initiated from a user and received at the electronic appliance (the Information Consumer 30).” *Id.* at 38 (citing Ex. 1002 ¶¶ 83, 109–111, 119).

In its Response, Intertrust argues that Dolby’s argument is inconsistent with its argument for limitation 4c, which maps actions of information consumer 30 to Narasimhalu’s access device, whereas for limitation 4d, Intertrust argues that Dolby maps the actions of information consumer 30 to a separate device that must present the COIN and the opener to controller 48. *See* PO Resp. 30–32 (citing Ex. 1004, 10:24–31; Ex. 2024 ¶¶ 86–88).

In its Reply, Dolby disagrees that its argument for limitation 4d is inconsistent with its argument for 4c, because Dolby “consistently references the Consumer (computing device) as the electronic appliance.” Pet. Reply 16 (citing Pet. 31, 36, 38).

In its Sur-reply, Intertrust argues that, if Dolby’s contention that information consumer 30 is the access device is correct, then “[information consumer 30’s] presentation of the Opener and COIN to the Access Device is, at best, an internal process *within* the electronic appliance, not a request received ‘*at* the electronic appliance.’” PO Sur-reply 7.

We disagree with Intertrust that Dolby’s argument for limitation 4d is inconsistent with its argument for limitation 4c. It is clear from the Petition that Dolby regarded operations by information consumer 30 as being performed by the access device. *See* Pet. 31 (stating that “receiving, at the electronic appliance” constitutes “receiving information . . . at Information Consumer 30 through a computer network”).

We also disagree with Intertrust’s argument, in its Sur-reply, that Narasimhalu’s process cannot meet limitation 4d if it is an “internal process”

within the electronic appliance. Limitation 4d requires that the request is received “*at the electronic appliance.*” Ex. 1001, 314:32 (emphasis added). Thus, Intertrust’s contention amounts to a claim construction argument about the meaning of “at.” But Intertrust does not point to any evidence supporting this interpretation, and does not explain why an operation occurring “at” a component of the electronic appliance does not also occur “at” the electronic appliance itself. *See* PO Sur-reply 7.

We note that limitation 4d does not explicitly specify who or what the request to use the electronic appliance is *from*, and does not explicitly indicate that the request cannot be from software or hardware within the electronic appliance itself. Based on the plain and ordinary meaning of limitation 4d, we find Dolby’s argument persuasive. Even though controller 48 is the specific component receiving the request, controller 48 is part of the electronic appliance, so receiving at controller 48 is also receiving “at the electronic appliance.” *See* Pet. 37; Ex. 1004, Fig. 6.

For the above reasons, we find that Dolby has shown that Narasimhalu discloses limitation 4d.

(f) Limitation 4e

Limitation 4e recites “determining that the requested use of the electronic content item corresponds to a permitted use of the electronic content item specified in the rule.” Ex. 1001, 314:34–36. Dolby argues that Narasimhalu discloses this limitation by “checking whether the LAD of the Opener matches the information consumer’s identification,” and by “verifying whether the current time is within the AWs specified in the Opener.” Pet. 38 (citing Ex. 1004, 11:13–30; Ex. 1002 ¶¶ 112–113, 119).

Intertrust does not contest Dolby's contentions regarding limitation 4e. We find Dolby's arguments and supporting testimonial evidence persuasive.

(g) Limitation 4f

Limitation 4f recites "using, at least in part, a decryption key to decrypt the electronic content item, the decryption key being stored in a secure processing unit contained in the electronic appliance." Ex. 1001, 314:37–40. Dolby argues, and Intertrust does not dispute, that Narasimhalu discloses using a decryption key for decrypting the electronic item. *See* Pet. 38–39 (citing Ex. 1004, 11:13–49; PO Resp. 38–39 (not addressing this issue)). We find Dolby's uncontested argument persuasive.

Dolby also argues that Narasimhalu discloses storing its decryption keys in a secure processing unit (SPU) in its "tamper-proof Access Device, which includes controller 48 and memory storage 52." Pet. 39–40 (citing Ex. 1004, 7:3–6, 7:27–29, 8:51–59; Ex. 1002 ¶¶ 114–116). To the extent that Narasimhalu does not explicitly disclose storing the keys in the access device, Dolby contends that Chorley supplies this teaching, as we discuss above in part III.C.3. Pet. 40–42 (citing Ex. 1006, 1:51–2:8, 2:36–51, 4:5–12, 5:23–32, 6:12–25, 6:41–42; Ex. 1002 ¶¶ 84, 90–93, 117–119).

In its Response, Intertrust does not contest "whether Narasimhalu alone or in combination with Chorley teaches or renders obvious to a [person of ordinary skill in the art] that a decryption key could be *stored* in Narasimhalu's access device." PO Resp. 38. Rather, Intertrust argues that Dolby has not shown that Narasimhalu discloses a "secure processing unit" according to the agreed construction "processing unit that makes information and processes resistant to unauthorized use." *Id.* at 38 & n.11. Intertrust

notes that this construction requires that the “processing unit” and “processes” are resistant to unauthorized use, and argues that Dolby has only shown that Narasimhalu’s access device has tamper-proof “channels,” coupled to controller 48, that prevent access to memory storage 52, or clock 55. *See id.* at 39 (citing Ex. 1004, 2:62–65, 8:55–59). According to Intertrust, “[t]hese features to not make the controller 45/48, itself, or the information and processes it executes, resistant to unauthorized use.” *Id.* (citing Ex. 2024 ¶ 96); *see also* PO Sur-reply 11–12 (reiterating its contention that Narasimhalu only discloses tamper-proofing with respect to the channels coupled to the controller, and not the controller itself).

In its Reply, Dolby argues that “Narasimhalu discloses that it is ‘impossible for users to tap into the clear channel 47, to access the Controller 48, to alter the value of the memory storage 52, or to change the value of the clock 55.’” Pet. Reply 18 (citing Ex. 1004, 8:55–59). Thus, Dolby contends that Narasimhalu *does* disclose that controller 48 and its processes are resistant to unauthorized access. *See id.* at 18–19.

We find Dolby’s argument persuasive. Although Narasimhalu focuses on making the “channels” tamper-proof, this has the result, as Narasimhalu states, of “mak[ing] it impossible for users . . . to access the Controller 48.” Ex. 1004, 8:57–58. Thus, we agree that Narasimhalu’s Access Device is a processing unit that makes information and processes resistant to unauthorized use, and is therefore a “secure processing unit” according to the parties’ agreed construction.

For the above reasons, we find that Dolby has shown that Narasimhalu teaches limitation 4f in light of the teachings of Chorley.

5. *Alleged Objective Indicia of Nonobviousness*

In its Response, Intertrust contends that there is evidence of long-felt need, failure of others, industry praise, commercial success, and copying which should be considered as objective indicia of nonobviousness.

PO Resp. 63–67.

For us to give substantial weight to objective indicia of obviousness or nonobviousness, a proponent must establish a nexus between the evidence and the merits of the claimed invention. *ClassCo, Inc. v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016). “[T]here is no nexus unless the evidence presented is ‘reasonably commensurate with the scope of the claims.’” *Id.* (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)).

A patentee is entitled to a presumption of nexus “when the patentee shows that the asserted objective evidence is tied to a specific product and that product ‘embodies the claimed features, and is coextensive with them.’” *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). But as Dolby correctly argues (Pet. Reply 28–30), a presumption of nexus is inappropriate here because Intertrust does not provide an analysis demonstrating that its products are coextensive (or nearly coextensive) with the challenged claim. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020) (precedential).

But even without the presumption, Intertrust “is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention.’” *Fox Factory*, 944 F.3d at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). Also, the nexus must be “to

some aspect of the claim *not already in the prior art.*” *In re Kao*, 639 F.3d 1057, 1069 (Fed. Cir. 2011) (emphasis added). “Ultimately, the fact finder must weigh the [objective indicia] evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan.” *Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331–32 (Fed. Cir. 2016)).

As we discuss below, we find that Intertrust has not shown a nexus between the claimed invention and long-felt need, failure of others, industry praise, commercial success, or copying. Although Intertrust comes closest to showing a nexus for industry praise, even if we were to find that there is a nexus, the evidence of industry praise is insufficient to outweigh the other evidence considered as part of the *Graham* factors.

Moreover, in addition to this proceeding, Intertrust presents nearly the same arguments and evidence with respect to objective indicia of nonobviousness in at least three other proceedings involving different patents. *See Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00662, Paper 17 at 60–65 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00664, Paper 15 at 63–66 (PTAB March 2, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-01123, Paper 18 at 42–45 (PTAB Apr. 20, 2021) (Patent Owner Response). Intertrust, however, does not explain adequately how the same evidence of objective indicia of nonobviousness can be attributable to each particular claimed invention. *See Fox Factory*, 944 F.3d at 1378 (“The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features. In such situations, the patentee retains the burden

of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention.” (citation omitted)).

(a) Long-Felt Need and Failure of Others

As evidence of long-felt need and failure of others, Intertrust submits three articles from the *Wall Street Journal* which, according to Intertrust, suggest a need for a way to distribute digital content in a secure manner that would “(1) ensure the digital content would only be used in an authorized manner, (2) ensure that the digital content creator would be compensated for use of the digital content, and (3) allow for such distribution to client devices that were not under the control of the distributor.” PO Resp. 63 (citing Ex. 2029, 1; Ex. 2030, 1; Ex. 2031, 1). Intertrust also submits another article from the *Wall Street Journal*, and an article from the *New York Times*, describing work by Xerox PARC, IBM, Microsoft, and other companies in the area of digital rights management. *Id.* at 64 (citing Ex. 2032, 3; Ex. 2033, 1).

Intertrust contends that “most, if not all, systems developed by others were either not commercially successful, were not adopted by digital content industries, copied the claimed invention or have been licensed under the claimed invention.” PO Resp. 64. But Intertrust does not cite any evidence supporting this argument.

We assign this evidence little weight, because Intertrust has not identified anything in the cited articles that ascribes any long-felt need to the merits of the claimed invention of the ’158 patent, and has not pointed to any evidence that others had failed to achieve a solution to any technical problem for which the invention of claim 4 is also a solution.

(b) Industry Praise

As evidence of industry praise, Intertrust submits an article in *IAM*, dated September 13, 2019, listing the patent family that includes the '158 patent as the most valuable patent family, based on a patent value index created by Unified Patents. PO Resp. 65 (citing Ex. 2034, 1–2). According to Intertrust, “[t]he existence of nexus is a foregone conclusion because the praise is for the *patent* (family) itself, not for a product (where there could be uncertainty as to whether the product incorporates the patented invention).” PO Sur-reply 25.

We disagree that Intertrust has shown a nexus or that there is a presumption of nexus, because the IAM article refers to the value of the patent family as a whole, not the value of the '158 patent or claim 4. Also, Intertrust has not identified anything in the IAM article that ascribes the value of this patent family to any aspect of claim 4, much less any aspect that was not already in the prior art. *See Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *Kao*, 639 F.3d at 1068–69). Thus, we assign this evidence little weight.

Also as evidence of industry praise, Intertrust submits two articles published in *Fortune*. PO Resp. 66–67 (citing Exs. 2035, 2036). Intertrust argues that the first article praises Intertrust technology for “wrap[ping] the file in a secure digital container and tag[ging] it with rules describing how it could be used,” and where, “[t]o play or read the . . . file, recipients would need special software or hardware that could be trusted by the content originator to enforce the rules.” *Id.* at 66 (alterations and omission in original) (emphasis omitted) (quoting Ex. 2035, 2). Intertrust contends that the second article praises “how Intertrust’s technology allows a record

company to let a customer ‘hear a song once free or three times for 25 cents’ or ‘for \$1.50, it might authorize you to download a copy of the song into your PC.’” *Id.* at 67 (quoting Ex. 2036, 2). According to Intertrust, the praise from these two articles relates to the use of “rules and controls,” and the use of a secure processing unit to “store a decryption key that is used to decrypt the content item.” *Id.* at 66–67 (emphasis omitted); *see also* PO Sur-reply 25 (citing Ex. 2035, 2) (arguing that the first article specifically describes a unique combination of features that includes rules and hardware that can be trusted by the content originator to enforce the rules).

In its Reply, Dolby contends that these features (rules and trusted enforcement via special software or hardware) already existed in the prior art, and thus cannot be the basis of a nexus to claim 4. *See* Pet. Reply 30.

We agree with Dolby that the *Fortune* articles fail to provide a nexus to the claimed invention. In this proceeding, Intertrust does not contest Dolby’s argument that Narasimhalu discloses rules (i.e., the opener). *See* PO Resp. 21–29. Although Intertrust contends that Narasimhalu fails to disclose a “processing unit that makes information and processes resistant to unauthorized use,” *Id.* at 55–57, the *Fortune* articles praise something somewhat different that Narasimhalu clearly discloses: “special software or hardware that could be trusted by the content originator to enforce the rules,” Ex. 2035, 2; *see* Ex. 1004, code (57) (“The end user accesses the digital information with a tamper-proof controlled information access device Controlled digital information will be accessed as long as the conditions specified by the information provider are met.”). Also, Intertrust concedes that the *Fortune* articles do not include praise for the idea that control

information is received independently via separate delivery, as recited in limitation 4c. *See* PO Sur-reply 25–26.

Thus, we find that Intertrust has not shown that there is a nexus between the evidence of industry praise and the merits of the claimed invention. Absent a nexus, we assign little weight to the evidence of industry praise. However, even if we were to assume there is a nexus between the *Fortune* articles and the merits of the claimed invention, this industry praise would not outweigh the other evidence considered as part of the *Graham* factors, including the evidence, addressed above, which shows that Narasimhalu, in light of Chorley, discloses all the limitations of claim 4, including a “rule” and a “secure processing unit.”

(c) Commercial Success and Copying

As evidence of commercial success and copying, Intertrust argues that over two dozen companies have licensed the claimed invention, and that “Intertrust has received more than \$1 billion in patent licensing revenue in return for granting licensees the right to practice the claimed invention and Intertrust’s remaining patent portfolio.” PO Resp. 67.

But Intertrust does not cite any evidence to support its contention, such as the mentioned licenses themselves, or any testimony by someone who was familiar with the circumstances of the licenses to Intertrust’s portfolio. Absent such evidence, we cannot assess whether the licenses have any nexus to claim 4. Thus, we assign little weight to Intertrust’s unsupported arguments on commercial success and copying.

6. *Conclusion*

Having considered the arguments and evidence presented by Dolby, Intertrust's responsive arguments and evidence, and the *Graham* factors including evidence about alleged objective indicia of nonobviousness, we determine that Dolby has shown, by a preponderance of the evidence, that claim 4 would have been obvious over the combination of Narasimhalu and Chorley, and is thus unpatentable.

D. GROUND BASED ON KATZNELSON AND CHORLEY

For its second ground, Dolby alleges that claim 4 is unpatentable under § 103(a) as obvious over Katznelson in view of Chorley. Pet. 8, 42–67. Based on the *Graham* factors, we determine that Dolby has *not* shown that claim 4 is unpatentable on this ground. We discuss the reasons below, after an overview of Katznelson.

1. *Overview of Katznelson*

Katznelson describes a “system for controlling and accounting for retrieval of data from a memory containing an encrypted data file from which retrieval must be authorized.” Ex. 1005, 1:13–16. The system has two parts that communicate with each other, as shown in Figure 1, reproduced below:

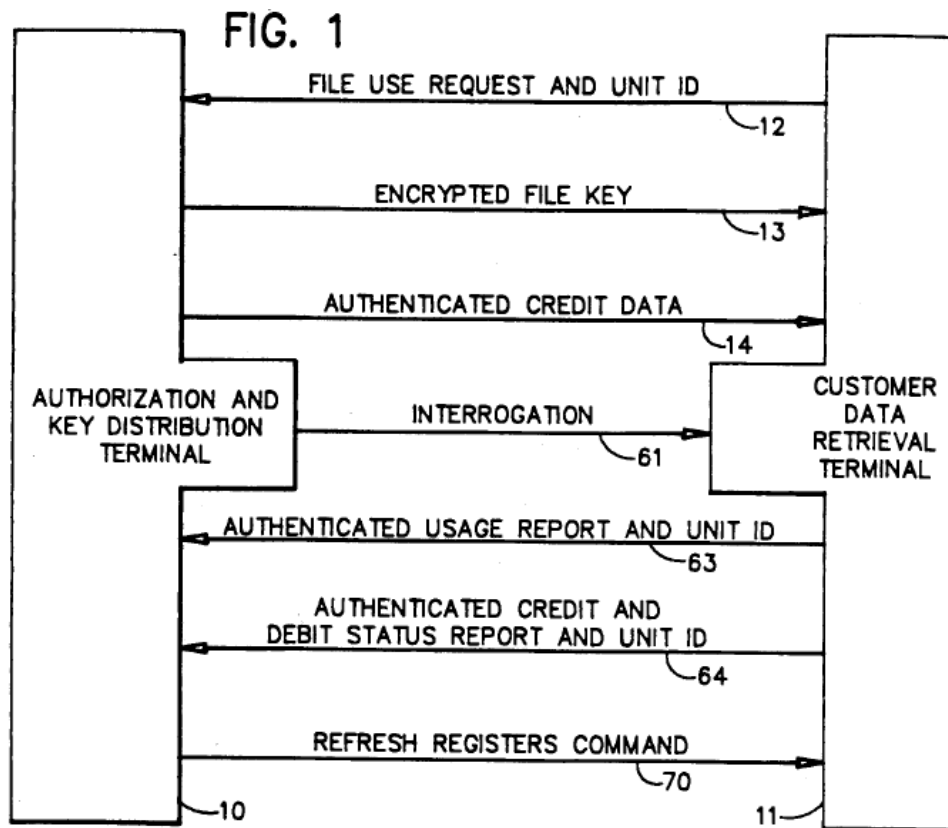


Figure 1, above, depicts “an authorization and key distribution terminal 10 and a customer data retrieval terminal 11,” of which there may be many communicating with authorization and key distribution terminal 10.

Ex. 1005, 1:61–66.

Customer data retrieval terminal 11 has access to a memory containing an encrypted data file, but does not initially have access to it because it is encrypted. *See* Ex. 1005, 1:66–2:1, 3:6–9. “In order to gain authorization to retrieve encrypted data from a given file stored in the memory,” customer data retrieval terminal 11 sends file use request signal 12, over a telephone line, to authorization and key distribution terminal 10. *Id.* at 2:5–11. This request identifies the file and the particular customer data retrieval terminal 11 that is making the request. *Id.* at 2:11–15. If the request is authorized, authorization and key distribution terminal 10 sends back

encrypted file key 13 and authenticated credit data signal 14. *Id.* at 2:16–35. “The credit data signal 14 indicates an amount of credit to be extended to the customer terminal 11 for retrieval of data from the file” stored in the memory. *Id.* at 2:35–38. Later, customer data retrieval terminal 11 may generate and send usage and credit reports back to authorization and key distribution terminal 10 (63, 64). *See id.* at 3:7–21.

Figure 2, reproduced below, illustrates customer data retrieval terminal 11:

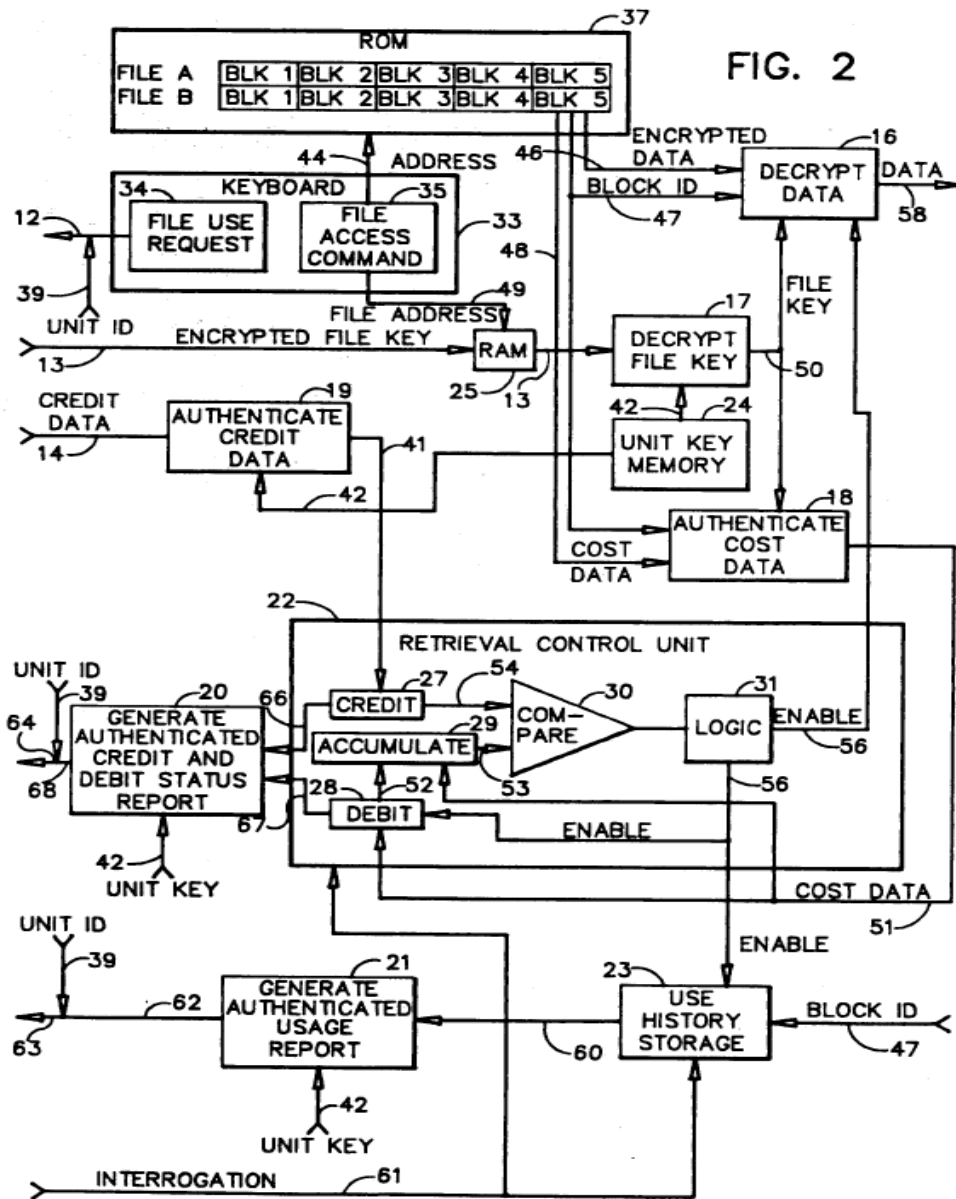


Figure 2 is “a functional block diagram of [a] customer data retrieval terminal.” Ex. 1005, 1:38–39. This customer data retrieval terminal 11 has several functional units “implemented in a microcomputer,” including “data decryption unit 16” and “a retrieval control unit 22 associated with each data vendor,” which is indicated in Figure 2 by a box containing other functional elements including “a credit register 27, a debit register 28, an accumulator 29, a comparator 30 and a logic unit 31.” *Id.* at 2:58–3:2.

Loaded into customer data retrieval terminal 11 is also read only memory (ROM) 37, which stores the encrypted data files (e.g., Files A and B). Ex. 1005, 3:6–9. Alternatively, the storage medium for the data can be a CD-ROM. *See id.* at 9:3–9, Fig. 6. Each data file in the ROM or CD-ROM contains several encrypted data blocks, each of which includes “authenticated cost data [that] indicates the cost associated with retrieving the given encrypted block of data.” *Id.* at 3:9–19. This cost for each data block is reflected in cost data signal 48, which the terminal authenticates to create authenticated cost data signal 51, which is an input to cost retrieval control unit 22. *See id.* at 4:11–21.

This embodiment of customer data retrieval terminal 11 also contains keyboard 33, through which the user sends file use request signal 12 over a telephone line to authorization and key distribution terminal 10. Ex. 1005, 2:3–15, 3:20–26. As discussed above, authorization and key distribution terminal 10 responds to file use request signal 12 by sending back to the customer data retrieval terminal 11 encrypted file key 13 and credit data signal 14. *Id.* at 3:26–35. Each customer data retrieval terminal 11 has a unique unit key 42, stored in unit key memory 24, which is used to decrypt file key 13 and to authenticate credit data signal 14. *Id.* at 2:48–49, 3:40–45. Once authenticated, credit data signal 14 (now identified as authenticated credit data signal 41) becomes an input to retrieval control unit 22, and is stored in credit register 27. *Id.* at 3:45–46.

In retrieval control unit 22, cost data signal 48/51 is added to the sum of previous cost data signals (which are accumulated in debit register 28) and compared with accumulated credit signal 54 (which is the accumulated sum of cost data signals 14/41) “to determine whether the customer terminal

. . . has been credited with sufficient credit to authorize retrieval of data from the requested file.” Ex. 1005, 4:30–33. “When the compensation indicates that there is sufficient accumulated credit to authorize such retrieval,” retrieval control unit 22 generates enable signal 56, which allows customer data retrieval terminal 11 to decrypt the file data in decryption unit 16. *Id.* at 4:33–37, 4:44–45.

2. *Analysis*

For limitation 4c, Dolby contends that Katznelson “discloses receiving, at the electronic appliance, a rule specifying one or more permitted uses of the electronic content item.” Pet. 55. Dolby contends that this “rule” is Katznelson’s credit data signal 14, which is “a permission to use the requested file for the credited amount.” Pet. 55–56.

In its Response, Intertrust argues that the language of limitation 4c “plainly requires that the ‘rule’ *affirmatively recite* the parameters for permitted uses.” PO Resp. 44 (citing Ex. 2024 ¶ 103). According to Intertrust, Katznelson does not affirmatively recite any permitted uses, and at best, the particular allowed uses associated with credit data signal 14 are *implied* rather than affirmatively specified. *See id.* at 44–45 (citing Ex. 1005, 2:35–36, 3:49–51; Ex. 2024 ¶ 104); *see also* PO Sur-reply 18–20.

We agree. By its ordinary and customary meaning, the phrase “rule specifying one or more permitted uses of the electronic content item” requires that the rule, itself, must specify at least one permitted use. In its Petition, Dolby does not explain how Katznelson’s credit data signal 14 specifies such a use. Pet. 42–51, 55–60.

In its Reply, Dolby argues that credit data signal 14 is a rule, and that a “rule,” as that term was construed in the Texas Actions, does not

necessarily require any particular syntax or format. *See* Pet. Reply 19–25. But this argument does not address the separate aspect of limitation 4c that the rule “specify[] one or more permitted uses of the electronic content item.” Ex. 1001, 314:30–31. Although a person of ordinary skill in the art might infer, after customer data retrieval terminal 11 receives credit data signal 14, that authorization and key distribution terminal 10 has granted permission to use parts of a digital file, Dolby has not shown how the rule itself “specif[ies]” this permission.

Because Dolby has not adequately explained or supported this aspect of limitation 4c in its ground based, in part, on Katznelson, we determine that Dolby has failed to “articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *Magnum Oil Tools*, 829 F.3d at 1380. And as a consequence, Dolby has not shown that claim 4 would have been obvious over the combination of Katznelson and Chorley.

IV. CONCLUSION⁷

For the reasons given above, Dolby has shown by a preponderance of the evidence that claim 4 of the ’158 patent is unpatentable, as summarized in the following table:

⁷ Should Intertrust wish to pursue amendment of claims in a reissue or reexamination proceeding after this decision, we draw Intertrust’s attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Intertrust chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Intertrust 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) (2020).

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
4	103(a)	Narasimhalu, Chorley	4	
4	103(a)	Katznelson, Chorley		4
Overall Outcome			4	

V. ORDER

In consideration of the foregoing, it is

ORDERED that claim 4 of the '158 patent is unpatentable;

FURTHER ORDERED that parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2020-00661
Patent 8,191,158 B2

For PETITIONER:

Scott McKeown
Mark Rowland
Victor Cheung
ROPES & GRAY LLP
Scott.mckeown@ropesgray.com
Mark.rowland@ropesgray.com
Victor.cheung@ropesgray.com

Leslie Spencer
KILPATRICK TOWNSEND & STOCKTON LLP
lspencer@desmaraisllp.com

For PATENT OWNER:

Christopher Mathews
Razmig Messerian
Tigran Guledjian
Scott Florance
QUINN EMANUEL URQUHART & SULLIVAN LLP
chrismathews@quinnemanuel.com
razmesserian@quinnemanuel.com
tigranguledjian@quinnemanuel.com
scottflorance@quinnemanuel.com